

**Social Security Number Protection Task Force**  
Report to the Illinois General Assembly, Governor Rod R. Blagojevich,  
and Secretary of State Jesse White  
December 31, 2008

**CONTENTS**

- I. Task Force Background
  - a. Membership of the Task Force
  - b. Groups that participated in Task Force meetings
- II. Task Force Meeting, September 18, 2008
  - a. Part I: Protection of SSNs in the Public Record
    - i. Federal Protections of SSNs
    - ii. State Legislative Update
    - iii. Redaction of SSNs from Public Documents
    - iv. SSNs in Court Documents
    - v. Information Security Programs
  - b. Part II: SSNs as Internal Identifiers
    - i. State and Local Agency Implementation of Unique Identifiers
    - ii. Agency Assessments of Internal SSN Use
    - iii. Progress in Other States
- III. Task Force Appointments
- IV. Conclusion

**APPENDICES**

- Appendix 1 *Social Security Numbers are Widely Available in Bulk and Online Records, but Changes to Enhance Security are Occurring* (GAO Report, September 2008)
- Appendix 2 *Security in Numbers: SSNs and ID Theft* (Federal Trade Commission Report, December 2008)
- Appendix 3 *Information Security Policy* (City of Chicago, February 15, 2008)
- Appendix 4 *Attorney General Security Breach Notification Guidance* (Vermont Attorney General's Office, April 24, 2007)
- Appendix 5 *The Beacon View* (State of North Carolina Office of the State Controller newsletter, Summer 2007)

## TASK FORCE BACKGROUND

Although the Social Security number (SSN) was intended to be used for the limited purpose of distributing Social Security benefits to eligible individuals, it is now used as an identifier for a wide range of purposes. Documents that contain an individual's SSN can be very valuable to an identity thief. According to the President's Identity Theft Task Force Report, issued in April 2007, "[c]onsumer information is the currency of identity theft, and perhaps the most valuable piece of information for the thief is the SSN." As incidents of identity theft continue to harm Illinois consumers, the need to protect the SSN and prevent its continued widespread dissemination is paramount.

The General Assembly created the Social Security Number Protection Task Force (Task Force) through Public Act 93-0813 in 2004. The Task Force is charged with examining the procedures used by the State to protect an individual against the unauthorized disclosure of his or her SSN when the State requires the individual to provide that number to an officer or agency of the State. The Task Force also is required to explore the technical and procedural changes that are necessary to implement a unique identification system to replace the use of SSNs by State and local governments for identification and record-keeping purposes. In 2007, the General Assembly amended the law governing the Task Force by Public Act 95-0482. The new law places the Task Force within the Office of the Attorney General (OAG) and requires the OAG to administer the activities of the Task Force. This law took effect on August 28, 2007.

The Task Force brings together representatives from many state agencies and constitutional offices to address these timely issues, and ultimately recommend rules, regulations or legislation that will prevent the further dissemination of SSNs.

### Membership of the Task Force:

- Two members representing the House of Representatives, appointed by the Speaker of the House – **Representative John Fritchey and Representative Sara Feigenholtz**
- Two members representing the House of Representatives, appointed by the Minority Leader of the House – **Representative Ruth Munson, Representative Sandra Pihos**
- Two members representing the Senate, appointed by the President of the Senate – **Senator Jeffrey Schoenberg, Senator Jacqueline Collins**
- Two members representing the Senate, appointed by the Minority Leader of the Senate – **Senator Chris Lauzen, TBA**
- One member representing the Office of the Attorney General – **Deborah Hagan, Task Force Chair**
- One member representing the Office of the Secretary of State – **Micah Miller**
- One member representing the Office of the Governor – **Martin Cohen**
- One member representing the Department of Natural Resources – **J.J. Pohlman**
- One member representing the Department of Healthcare and Family Services – **Tamara Hoffman**
- One member representing the Department of Revenue – **George Logan**
- One member representing the Department of State Police – **TBA**
- One member representing the Department of Employment Security – **Joseph Mueller**
- One member representing the Illinois Courts – **James Morphew**

- One member representing the Department on Aging – **Patricia Carter**
- One member representing Central Management Services – TBA
- One member appointed by the Executive Director of the Board of Higher Education – **Don Sevener**
- One member appointed by the Secretary of Human Services – **Solomon Oriakhi**
- Three members representing local-governmental organizations – **Dorothy Brown, Larry Reinhardt, Virginia Hayden**
- One member representing the Office of the State Comptroller – **Whitney Rosen**
- One member representing school administrators, appointed by the State Superintendent of Education – **Sara Boucek**

Groups that participated in Task Force meetings:

- The Illinois Municipal League
- The Association of County Clerks and Records
- The University of Illinois
- The Illinois Bankers Association
- The Illinois Community College Board
- The Metro Counties Association
- The Township Officials of Illinois
- The City of Chicago

**TASK FORCE MEETING, SEPTEMBER 18, 2008**

On Thursday, September 18, 2008, the Task Force convened at the Office of the Attorney General in Springfield. Some of the Task Force members participated in the meeting via conference call. Interested parties who are not official members of the Task Force participated as well.

Those participating in the meeting included:

Representative Ruth Munson  
 Representative Sandy Pihos  
 Representative Sandy Cole  
 Deborah Hagan, Office of the Attorney General (Task Force Chair)  
 Elizabeth Blackston, Office of the Attorney General  
 Christine Nielsen, Office of the Attorney General  
 Mindy Summers, Office of the Attorney General  
 Micah Miller, Secretary of State's Office  
 George Logan, Department of Revenue  
 Fred Baird, Illinois Department of Employment Security  
 Whitney Rosen, Comptroller's Office  
 David Smalley, Illinois Board of Higher Education  
 Matt Davidson, Illinois Municipal League  
 Kip Kolkmeier, Metro County Association  
 Lee Newcom, McLean County Recorder  
 Paul Frank, Private Colleges & Universities  
 Scott Selinger, Illinois Bankers Association

Larry Reinhardt, Jackson County Recorder  
Jenny Hayden, Quincy City Clerk  
Suzy Choi, Cook County Court Clerk's office  
John Hollman, Speaker Madigan's staff  
Brittan Bolin, Illinois Association of Court Clerks  
Rob Karr, Illinois Retail Merchants Association

## Part I: Protection of SSNs in the Public Record

The first statutory requirement of the Social Security Number Protection Task Force Act is to examine the procedures used by the State to protect an individual against the unauthorized disclosure of his or her Social Security number (SSN).

### *Federal Protections of SSNs*

The President's Identity Theft Task Force was created in 2006 by executive order that charged 15 federal departments and agencies with crafting a comprehensive national strategy to more effectively combat the crime of identity theft. The Task Force submitted a Strategic Plan in 2007, and more recently, in September 2008, released a follow-up report. The Strategic Plan recommended that agencies study the private sector uses of SSNs, develop a deeper understanding of the relationship between the SSN and identity theft, and take steps to decrease the unnecessary use of SSNs. The follow-up report from 2008 provided updates on what federal agencies have done to reduce the unnecessary use of SSNs.

First, agencies were asked to complete a review of their current use of SSNs. The Office of Personnel Management (OPM) has developed and begun implementation of a plan to reduce unnecessary uses of SSNs. OPM is also studying the feasibility of using a unique identification number in place of the SSN. Agencies were also asked to issue guidance on the appropriate uses of SSNs. On June 18, 2007, OPM issued "Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft" to all federal departments and agencies.

In response to the recommendation to require agencies to review use of SSNs, the Office of Management and Budget (OMB) reviewed a government-wide survey on the use of SSNs and issued a memorandum titled "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." Agencies, with OMB guidance, have taken steps to reduce the unnecessary collection and use of SSNs.

As part of its ongoing efforts to assess the availability and use of SSNs in public and private sectors, the federal government in 2008 required the Government Accountability Office (GAO) to examine the availability of SSNs for bulk purchase and online, and to review what measures may be in place to protect SSNs in those records. The GAO surveyed a sample of 247 counties in 45 states and the District of Columbia. Results in Brief (from *Social Security Numbers are Widely Available in Bulk and Online Records, but Changes to Enhance Security are Occurring*, GAO Report, September 2008):

- 85% of the largest counties make records with full or partial SSNs available in bulk or online compared with 41% of the smallest counties.
- Counties cited state laws as the primary reason for making records available.

- Counties generally do not control how records are used; 16% of counties that make records available online place restrictions on the types of entities that can obtain the records.
- Title companies are the most frequent recipients of records, but mortgage companies and data resellers obtain records as well.
- Businesses that obtain public records may have safeguards in place to secure the information.
- In some cases, information in the public records is sent overseas for processing.
- 12% of counties have completed redacting or truncating SSNs that are in public records and 26% are in the process.

In December 2008, the Federal Trade Commission issued a report entitled *Security in Numbers: SSNs and ID Theft* in response to the President's Identity Theft Task Force's recommendations. The FTC report provides five recommendations to make SSNs less available to identity thieves and to make SSNs less valuable if and when they are accessed. The FTC's five recommendations are:

- Improve customer authentication;
- Restrict the public display and the transmission of SSNs;
- Establish national standards for data protection and breach notification;
- Conduct outreach to businesses and consumers; and
- Promote coordination and information sharing on use of SSNs.

#### *State Legislative Update*

During the September 18 meeting, Representative Munson provided the Task Force with a legislative update. House Bill 4219, the Identity Protection Act, remained in the Senate as of the end of the 2008 general session. That bill would require state and local governmental agencies to create, implement and maintain an Identity Protection Policy that includes procedures for segregating SSNs for easy redaction. The House of Representatives passed HB4219, but the bill did not advance out of committee in the Senate during the 2008 session.

In the 2008 session, Representative Schock introduced HB5562, which would have required clerks of court to take appropriate actions to redact or otherwise prevent the release of an individual's SSN contained on a document or record maintained by the clerk. Representative Munson reported that Representative Schock held the bill.

The General Assembly passed, and the Governor signed into law, a mandated plan of action for Recorders of Deeds. Under Public Act 095-0875, Recorders must file a written policy that includes a timetable for redaction of SSNs from records publicly displayed.

#### *Public Act 095-0875 (HB5586)*

Public Act 095-0875, effective January 1, 2009, amends the Counties Code by adding a new section 3-5047 regarding the removal of personal information. The amendment requires each recorder to remove, upon request, a person's Social Security number (SSN) from any website maintained by the recorder to display public records. In addition, by January 1, 2010, all county recorders must file with the General Assembly a written policy, including a timeline, for the redaction of SSNs from all records publicly displayed

on the website. No person shall include an individual's SSN in a document that is prepared and presented for recording, with exceptions.

#### *Redaction of SSNs from Public Documents*

Lee Newcom, McLean County Recorder, reported on the status of the McLean County redaction project. McLean County decided to close access to documents online. Access to public records online is now granted only through an application process. Land records remain open, but it is difficult to locate SSNs on those documents. McLean County just approved a contract to mask SSNs online, with an estimated cost of \$80,000.

Deborah Hagan, the Task Force Chair, sought comments on whether it would be feasible to amend state public records acts to require across-the-board redaction. Task Force members commented that it was important to weigh the cost of redaction against risk of identity theft, since incidences of identity theft have not been directly linked to SSNs in public records. In addition, any legislation must take into account the fact that there are certain documents that recorders cannot redact or alter at all, like federal tax liens. The group also discussed the industry practice of redacting the first 5 digits, and allowing the last 4 digits of the SSN to be displayed and used for identification and other purposes. The group discussed whether possible legislation should move away from this practice, since the last 4 digits are the only unique numbers in the SSN.

Cost is also an impediment to across-the-board redaction. First, a county must invest in software that can identify potential SSNs for redaction. Second, the county must invest in the training of staff to work with the software to review the results and correct any errors. The Task Force members discussed the feasibility of sharing cost of obtaining a software license and the cost of training consultants to participate in the process.

#### *SSNs in Court Documents*

Effective December 1, 2007, the Federal Rules of Civil Procedure were amended to offer more privacy protection for filings made in federal court. Under newly amended Rule 5.2, an electronic or paper filing made with the court that includes a SSN or an individual's tax identification number, a name of a person known to be a minor, a person's birth date, or a financial account number may include only: (1) the last four digits of the social security number and tax identification number; (2) the minor's initials; (3) the year of birth; and (4) the last four digits of the financial account number. There are several exemptions to the redaction requirement.

State court filings may contain SSNs in some circumstances, as well. The Task Force discussed whether Illinois state courts might implement a rule similar to the Federal Rule of Civil Procedure 5.2. The Task Force will follow up with the Administrative Office of the Illinois Courts to discuss available options for state court filings.

#### *Information Security Programs*

Under HB4219, all local and state government agencies would have been required to implement an internal program to better protect personal information maintained by the agencies. Although

the requirements of HB4219 are not law in Illinois, many local and state government agencies have begun creating and implementing such programs.

The Task Force Chair reported that the City of Chicago is one such agency that has implemented an Information Security Program. The Chair distributed copies of that program for review by Task Force members.

The Chair also reported that state agencies have an obligation under the Illinois Personal Information Protection Act to notify affected individuals in the event of a security breach. An Information Security Program can help a business or governmental agency prepare for such notification. Other states, such as California and Vermont, have provided guidance for complying with state breach notification laws. The Chair distributed copies of Vermont's guidance to the members. Task Force members expressed interest in Illinois-specific guidance. The OAG has begun drafting such guidance.

## Part II: SSNs as Internal Identifiers

The second requirement of the Task Force is to explore the technical and procedural changes that are necessary to implement a unique identification system to replace the use of SSNs for identification and record-keeping purposes by State and local governments.

### *State and Local Agency Implementation of Unique Identifiers*

The Illinois State Board of Education has implemented a unique identification number that follows students from kindergarten through higher education. Higher Education has worked with ISBE to integrate the number so that it appears on transcripts and follows the student throughout his/her education. The SSN has to be linked with the ISBE number. The two numbers appear together only in one place, and that location is locked down securely.

Micah Miller from the Secretary of State reported that SOS has begun implementation of an internal unique identifier for employees. Employees use that unique number for access to online training.

### *Agency Assessments of Internal SSN Use*

Although other agencies have considered implementing a unique identification number system, a threshold issue is an assessment of the collection and maintenance of SSNs. Some agencies have already begun this process.

Whitney Rose from the Comptroller's Office reported that her office has completed a confidential data assessment. The first step was to review information that comes into the office and ask whether the SSN was necessary for that function. If not, the Comptroller's Office has changed forms so that the SSN is not requested, and has begun asking the agency that submits the information to remove the number. The next steps for the Comptroller include assessing the use and transmittal internally; assessing the transmittal of information externally; and assessing the feasibility of unique identifier.

All agencies that have begun the process of replacing the SSN with an internal unique identification number indicate that the largest challenge is linking the SSN to that unique identifier in a secure way. For many reasons, those two numbers must be linked in at least one place.

#### *Progress in Other States*

The Chair reminded the Task Force the North Carolina has implemented a unique identification number system for state employees. The unique number has replaced the SSN on most paperwork. The Chair distributed copies of a North Carolina state newsletter that explained the implementation of the new system, which was part of a larger information technology upgrade.

#### **TASK FORCE APPOINTMENTS**

Many members of the Task Force were appointed soon after the Task Force became effective, but when the law was amended in 2007, more appointments became necessary. The following recent appointments have been made to the Task Force.

On September 4, 2008, the Chair appointed three members to the Task Force to represent local governmental organizations. The Chair appointed:

- Larry W. Reinhardt, Jackson County Clerk/Recorder. Mr. Reinhardt is currently serving his third term as Jackson County Clerk/Recorder and served as President of the Illinois Association of County Clerks and Recorders in 2007.
- Dorothy Brown, Clerk of the Circuit Court of Cook County. Clerk Brown is one of three appointees representing local-governmental organizations. Clerk Brown was elected to as the Clerk of the Circuit Court of Cook County in 2000 and again in 2004.
- Virginia N. Hayden, Quincy City Clerk. Ms. Hayden became Deputy City Clerk in 1989, and took over the role of City Clerk for the City of Quincy in 2003.

On October 31, 2008, the Executive Director of the Illinois Board of Higher Education appointed Don Sevener to the Task Force. Mr. Sevener is the Deputy Director for External Relations.

On November 17, 2008, the Secretary of the Illinois Department of Human Services appointed Solomon Oriakhi to the Task Force. Mr. Oriakhi is the Director of the Office of Fiscal Services.

On November 18, 2008, the Speaker of the House appointed Representatives John Fritchey and Sara Feigenholtz to the Task Force.

On November 19, 2008, the Director of the Illinois Department on Aging appointed Patricia Carter to the Task Force. Ms. Carter is the Chief Financial Officer.

#### **CONCLUSION**

The Task Force continues to bring together individuals from state and local governmental agencies who are invested in finding a solution to the widespread dissemination of Social Security numbers.



Appendix 1

*Social Security Numbers are Widely Available in Bulk and Online Records, but Changes to Enhance Security are Occurring* (GAO Report, September 2008)



United States Government Accountability Office  
Washington, DC 20548

September 19, 2008

The Honorable Charles E. Schumer  
Chairman  
Subcommittee on Administrative Oversight and the Courts  
Committee on the Judiciary  
United States Senate

*Subject: Social Security Numbers Are Widely Available in Bulk and Online Records, but Changes to Enhance Security Are Occurring*

Various public records in the United States contain Social Security numbers (SSN) and other personal identifying information that could be used to commit fraud and identity theft. For the purposes of this report, public records are generally defined as government agency-held records made available to the public in their entirety for inspection, such as property and court records. Although public records were traditionally accessed locally in county courthouses and government records centers, public record keepers in some states and localities have more recently been maintaining electronic images of their records. In electronic format, records can be made available through the Internet or easily transferred to other parties in bulk quantities. Although we previously reported on the types of public records that contain SSNs and access to those records, less is known about the extent to which public records containing personal identifying information such as SSNs are made available to private third parties through bulk sales. In light of these developments, you asked us to examine (1) to what extent, for what reasons, and to whom are public records that may contain SSNs available for bulk purchase and online, and (2) what measures have been taken to protect SSNs that may be contained in these records.

To answer these questions, we collected and analyzed information from a variety of sources. Specifically, we conducted a survey of county record keepers on the extent and reasons for which they make records available in bulk or online, the types of records that they make available, and the types of entities (e.g., private businesses or individuals) that obtain their records. We focused on county record keepers because, in scoping our review, we determined that records with SSNs are most likely to be made available in bulk or online at the county level. We surveyed a sample of 247 counties—including the 97 largest counties by population and a random sample of 150 of the remaining counties, received responses from 89

---

percent, and used this information to generate national estimates to the extent possible. Our survey covered 45 states and the District of Columbia, excluding five states where recording of documents is not performed at the county level (Alaska, Connecticut, Hawaii, Rhode Island, and Vermont). We used the information gathered in this survey to calculate estimates about the entire population of county record keepers.<sup>1</sup>

To obtain information on how businesses use information from public records, we identified and interviewed a judgmentally selected group of private businesses representing a cross section of industries that obtain records in bulk or online. Furthermore, we conducted site visits in Illinois, Texas, California, and the Washington, D.C. area to speak with county record keepers and businesses that obtain records in bulk or online. We visited these locations based on the large volume of records they maintain, as well as recent statutory and administrative efforts in those states to place limits on bulk transfers or the availability of SSNs in public documents. In addition, we interviewed interest groups we identified while planning our work that represent record keepers and businesses that utilize public records. We also reviewed relevant federal privacy and records laws and recently proposed legislation related to information privacy, reviewed state laws we identified from outside sources, and reviewed available information on select foreign data protection laws. We performed our work from September 2007 through September 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

On September 4, 2008, we briefed your staff on the results of our work. This letter formally conveys the information provided during that briefing

---

<sup>1</sup>Because we followed a probability procedure based on random selections, our sample is only one of a large number of samples that we might have drawn. Since each sample could have provided different estimates, we express our confidence in the precision of our particular sample's results as a 95 percent confidence interval (i.e., plus or minus 15 percentage points). This is the interval that would contain the actual population value for 95 percent of the samples we could have drawn. As a result, we are 95 percent confident that each of the confidence intervals in this report will include the true values in the study population. In addition, for reporting purposes, each sample element selected was subsequently weighted in the analysis to account statistically for all the members of the population.

---

(see enc. I). Concurrently with this letter, we are issuing an electronic supplement that shows the responses to all survey items.<sup>2</sup>

---

## Results in Brief

Many counties make public records that may contain Social Security numbers (SSNs) available in bulk to businesses and individuals in response to state open records laws, and also because private companies often request access to these records to support their business operations. Our sample allows us to estimate that 85 percent of the largest counties make records with full or partial SSNs available in bulk or online,<sup>3</sup> while smaller counties are less likely to do so (41 percent). According to county officials and businesses we interviewed, SSNs are generally found in certain types of records such as property liens and appear relatively infrequently. However, because millions of records are available, many SSNs may be displayed. Counties in our survey cited state laws as the primary reason for making records available, and requests from companies may also drive availability, as several told us they need bulk records to support their businesses models. Counties generally do not control how records are used. Of counties that make records available in bulk or online, only about 16 percent place any restrictions on the types of entities that can obtain these records. We found that title companies are the most frequent recipients of these records, but others such as mortgage companies and data resellers that collect and aggregate personal information often obtain records as well. Private companies we interviewed told us they obtain records to help them conduct their business, including using SSNs as a unique identifier. For example, a title company or data reseller may use the SSN to ensure that a lien is associated with the correct individual, given that many people have the same name. Information from these records may also be used by companies to build and maintain databases or resold to other businesses. Businesses we contacted told us they have various safeguards in place to secure information they obtain from public records, including computer systems that restrict employees' access to records. In some cases, information from these public records is sent overseas for processing, a practice referred to as offshoring. We were not able to determine the extent of offshoring, but both record keepers and large companies that obtain records in bulk told us that it is a common practice. In the course of our work, we found that public records data are commonly sent to at least two countries—India and the Philippines.

---

<sup>2</sup>GAO, *Social Security Numbers: Transfers and Sales of Public Records That May Contain Social Security Numbers, an E-supplement to GAO-08-1009R*, GAO-08-1004SP (Washington, D.C.: Sept 19, 2008).

<sup>3</sup>Unless otherwise noted, all estimates have a margin of error of 15 percent or less.

---

State and local governments, as well as the federal government, are taking various actions to safeguard SSNs in public records, but these actions are a recent phenomenon. Based on our survey, we estimate that about 12 percent of counties have completed redacting or truncating SSNs that are in public records—that is, removing the full SSN from display or showing only part of it—and another 26 percent are in the process of doing so. Some are responding to state laws requiring redaction or truncation, but others have acted on their own based on concerns about the potential for identity theft. For example, California and Florida recently passed laws that require record keepers to truncate or redact SSNs in their publicly available documents, while one clerk in Texas told us that in response to public concern about the vulnerability of SSNs to misuse, the county is redacting SSNs from records on its own initiative. In recent years, 25 states have enacted some form of statutory restriction on displaying SSNs in public records. Some states have also enacted laws allowing individuals to request that their SSNs be removed from certain records such as military discharge papers. For example, in one of the states we visited, we saw notices posted by county recorders describing the right to make this request. At the federal level, our prior work found that some federal agencies have taken action by truncating SSNs they place in the public record at the local level. For example, the Internal Revenue Service (IRS) recently started truncating SSNs in tax liens it files with local clerks and recorders, and the Department of Justice (Justice) initiated a similar practice for some liens and other records in response to our prior recommendations. However, we did not identify any federal laws restricting state or local governments from making public records available in bulk or governing how private entities may use SSNs obtained from public records, including the offshoring of records with SSNs. Although their governments have enacted measures that may address data security in the two countries where we were told public records data are sent, the extent to which those measures protect SSNs from inappropriate use is unclear. There are several bills pending in the current Congress that would limit both private and government entities' ability to sell or display SSNs to other parties. For example, one of the bills has a provision that would limit posting SSNs that are contained in public records on the Internet. The bills do not address how SSNs or personal information from public records that has been sent offshore should be handled.

---

## Concluding Observations

Recent actions by states and counties to limit the display of SSNs in records made available to the public through redaction or truncation are positive steps, but these actions will only protect SSNs in future transactions, as millions of records with SSNs have already been obtained in bulk or online. Additional concerns remain about the security of SSNs in these records. In particular, because many record keepers cannot or do not restrict what entities can obtain public records with SSNs or control

---

how they are used, and some businesses are sending records with SSNs offshore where little is known about how they are used or protected, ensuring the security of SSNs is an ongoing challenge.

In weighing how best to address some of these open issues over the availability of SSNs in public records, Congress will need to balance the need to keep SSNs confidential with the long standing tradition of open access to public records, the rights of states and localities to regulate the availability of records they maintain, and the use of SSNs in the private sector. Recent actions taken by the IRS, Justice, and states to truncate SSNs represent one effort that may strike an appropriate balance between protecting SSNs from misuse and making a portion available for appropriate parties to firmly establish the identity of specific individuals.

---

## Agency Comments

We provided a draft of this report to the Social Security Administration (SSA) and the Federal Trade Commission (FTC) for review and comment. SSA and FTC provided only technical comments which we incorporated as appropriate.

---

As agreed with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after its issue date. At that time, we will send copies of this report to relevant congressional committees, the Commissioner of SSA, the Chairman of FTC, and other interested parties and will make copies available to others on request. In addition, this report will be available at no charge on GAO's Web site at <http://www.gao.gov>. If you or your staff have any questions about this report, please contact me at 202-512-7215 or [bertonid@gao.gov](mailto:bertonid@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this study include Jeremy Cox (Assistant Director), Joel Marus (Analyst-in-Charge), Daniel Concepcion, and Jill Yost. In addition, Carolyn Boyce, Justin Fisher, Sheila McCoy, George Quinn, Walter Vance, and Charles Willson provided significant assistance.



Daniel Bertoni  
Director, Education, Workforce, and  
Income Security Issues

Enclosure

---

Enclosure I



---

# **Social Security Numbers Are Widely Available in Bulk and Online Records, but Changes to Enhance Security Are Occurring**

---

**Briefing for Senator Charles E. Schumer,  
Chairman, Subcommittee on Administrative  
Oversight and the Courts,  
Committee on the Judiciary**

**September 4, 2008**

---

## Overview

---

- Key Objectives
  - Scope and Methodology
  - Summary of Results
  - Background
  - Findings
  - Concluding Observations
-



## Key Objectives

---

The Chairman of the Senate Subcommittee on Administrative Oversight and the Courts, Committee on the Judiciary, requested that we conduct this study. We answered the following questions:

- To what extent, for what reasons, and to whom are public records that may contain Social Security numbers (SSNs) available for bulk purchase and online?
  - What measures have been taken to protect SSNs that may be contained in these records?
-

---

## Scope and Methodology

---

To answer these questions, we

- conducted a survey of county record keepers;
- interviewed companies from a cross section of industries that use public records for business purposes;
- visited county record keepers and businesses in Illinois, Texas, California, and the Washington, D.C., area; and
- interviewed organizations representing government public record keepers and organizations representing businesses that utilize public records.

## Scope and Methodology: Survey

- The survey was sent to offices in 247 counties responsible for recording documents—including the 97 largest counties by population and a random sample of 150 of the remaining counties. Overall response rate was 88.9 percent.
- AK, CT, HI, RI, and VT were omitted from our sample because document recording is not done at the county level.
- The survey was Web-based and was pretested prior to distribution.
- We used the information gathered in this survey to calculate estimates of the entire population of county record keepers. Unless otherwise noted, the margin of error for all estimates is 15 percent or less.

---

## **Scope and Methodology: Analysis of Laws to Protect SSNs**

---

- We reviewed relevant federal privacy and records laws and proposed legislation.
  - We reviewed select state statutory provisions identified through interviews and prior research conducted by the Social Security Administration, but did not conduct our own exhaustive search of state legal requirements.
  - Information on foreign laws in this report does not reflect our independent legal analysis, but is based on interviews and secondary sources.
-

## Summary of Results

- We estimate that 85 percent of large counties and 41 percent of small counties make records that may contain SSNs available in bulk or online.
- Counties cited state laws as a key reason for providing records. Generally, counties do not place restrictions on who obtains records or how they are used.
- Businesses obtain these records to use or resell data in them and may use SSNs to link identifying information on records back to specific individuals, such as ensuring that liens are applied to the correct individuals, since many people share the same name. In some cases, businesses send information from these records overseas for processing.

## Summary of Results (continued)

- Federal, state, and local governments have recently taken steps to safeguard SSNs in public records. We estimate more than a third of counties have already removed (redacted) or truncated SSNs or are currently removing SSNs from their records; some in response to state laws and others of their own accord.
- Some federal agencies have taken steps to remove full SSNs from documents they provide to counties. However, we did not identify any federal laws that appeared to restrict the bulk transfer of state and local public records or the display of SSNs in those records, nor did we identify any federal law that provides protections for SSNs obtained from public records and sent overseas by private parties. Several bills are pending in Congress that would limit the display or sale of SSNs to the public or to private entities.

## Background

- Although originally created to track workers' earnings and Social Security benefits, SSNs have become the universal identifier of choice for government agencies and are currently used for myriad non-Social Security purposes.
- The SSN's widespread use has also made it a key piece of information used to create false identities for financial misuse or to assume another individual's identity.
- The Federal Trade Commission (FTC) estimated that in 2005, 8.3 million people discovered they were victims of identity theft, translating into estimated losses of billions of dollars.

---

## **Background**

(continued)

---

- For purposes of this report, we define public records to include records or documents that are routinely made available to the public by a government agency or the courts.
  - There are many types of public records, including birth, death, and marriage records; criminal and civil court case files; and records that concern property ownership, such as property liens. The records are stored in formats such as paper, microfilm, and electronic image.
  - Public records that used to be accessible only in the county recorder's office can now be accessed electronically from other locations.
  - Some records contain personal identifying information, such as SSNs, dates of birth, and credit card or bank account numbers.
-



---

## **Background**

(continued)

---

- Individuals and businesses are able to obtain large numbers of public records. This generally involves the transfer of bulk or individual records:
    - Bulk: An entity (e.g., a private business or individual) obtains or buys all records held by a record keeper (such as property liens) and may receive regular updates, such as a weekly update of all such documents filed in the last week.
    - Individual: An entity obtains records one at a time, usually over the Internet, hereafter referred to as online. Service may be free or may require users to register and pay for access.
-

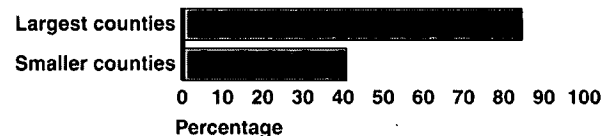
## Finding 1: Availability and use of records



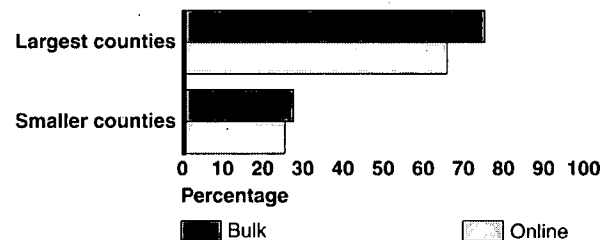
### Many Counties Make Records Available in Bulk or Online

- For the states covered by our survey,<sup>1</sup> we estimate that about 85 percent of large counties and 41 percent of small counties make records that may contain SSNs available in bulk or online.
- The 100 largest counties have a combined population of about 118 million.
- Some smaller counties indicated that they lack the resources to make records available in bulk or online.

Availability of Records That May Contain SSNs



Availability of Records That May Contain SSNs by Mode of Transfer



Source: GAO survey.

<sup>1</sup> This includes 45 states and the District of Columbia.

---

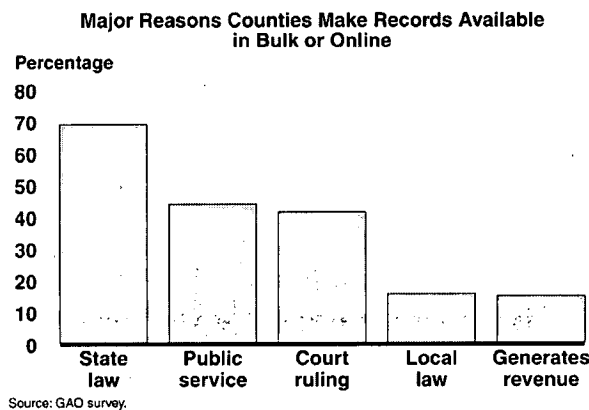
**While Record Keepers and Bulk Users Report SSNs Appear Relatively Infrequently in Records, the Total Number of Records with SSNs Could Be Large**

---

- Counties and businesses we interviewed told us:
  - SSNs generally appear more often in certain types of documents, including state and federal liens.
  - To a lesser extent, SSNs appear in judgments and mortgage records.
  - The prevalence of SSNs in documents is relatively low and has decreased over time.
- However, because record keepers can maintain millions of documents, many SSNs may be displayed.

## Counties Make Records Available for Various Reasons

- In our survey, counties cited requirements under state law as the most common major reason for making records available in bulk or online.



## **Demand from Businesses May Also Drive the Availability of Records**

- Several companies we interviewed said they need to obtain records in bulk to support their business models, such as developing a database of title records (known as a title plant).
- One title company told us that obtaining records in bulk increases the efficiency of its operations as opposed to having to physically travel to the recorder's office to search records.

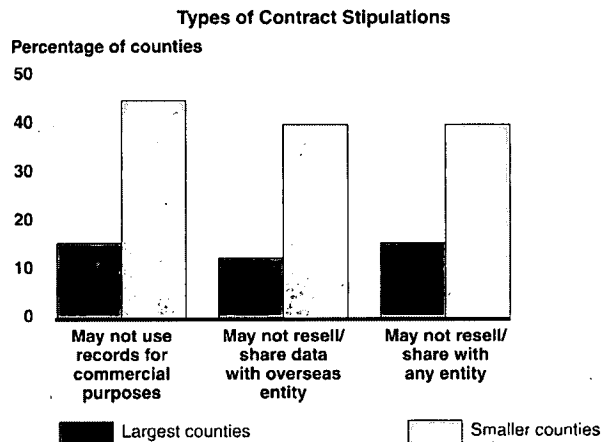
---

## **Counties Generally Do Not Place Restrictions on Who Obtains Records**

- We estimate that only about 16 percent of counties that make records available in bulk or online place some restrictions on the types of entities that can obtain records.
- Additionally, we estimate that only about 23 percent of counties that make records available in bulk or online take any steps to verify the identity of entities that obtain records.
- A majority of counties reported that there is no state or local law that requires or prohibits them from obtaining the identity of those who receive records in bulk or online.

## Counties Generally Do Not Control How Records Are Used

- We estimate that about 38 percent of counties require users of bulk or online records to enter into a contract or agreement.
- Among those counties, we found that smaller counties are more likely to have certain types of restrictions in place than are the largest counties.



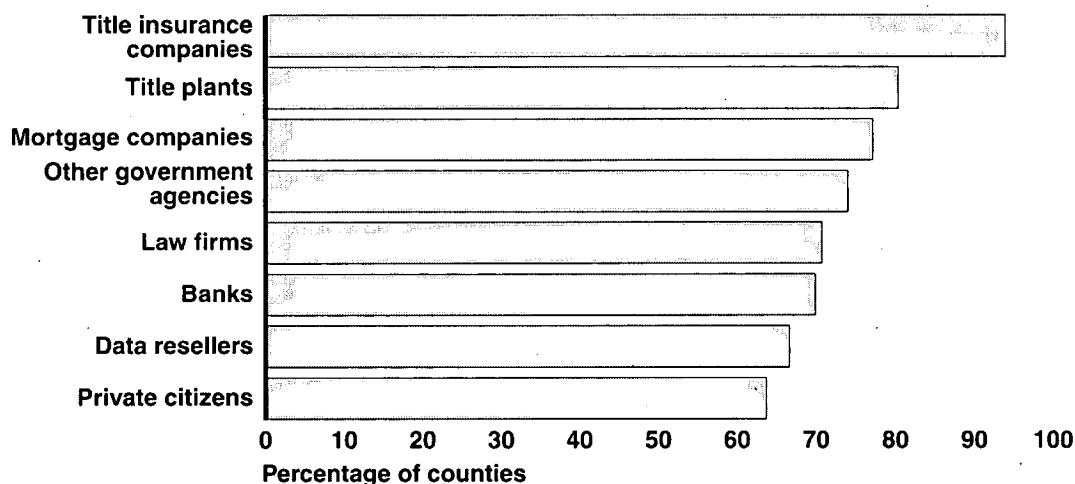
Source: GAO survey.  
Note: Confidence intervals for this chart range from 4.7 to 5 percent for the largest counties and 23.5 to 23.9 for smaller counties.

Finding 1: Availability and use of records



## Title Companies are the Most Common Recipients of Online or Bulk Documents

### Customers Obtaining Public Records



Source: GAO survey.

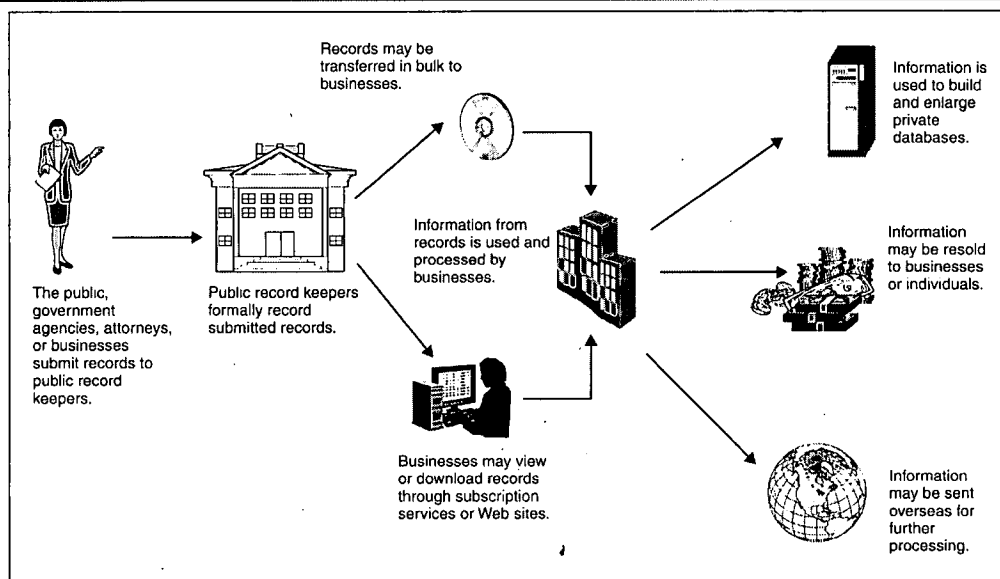
Note: Margins of error for this chart range from 9.6 to 19.1 percent.



Finding 1: Availability and use of records



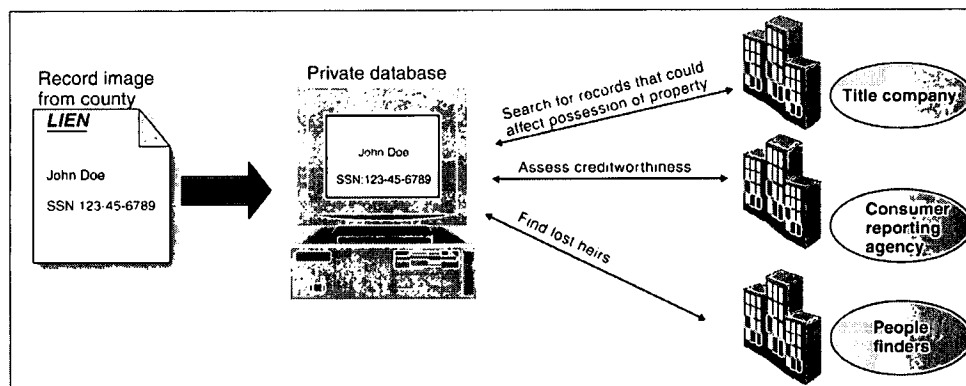
## Information from Public Records Can Change Hands Many Times



Sources: GAO, Ari Explosion (clip art)

## Businesses Use SSNs to Match Public Records Information to Specific Individuals

- Information from records is used by businesses, such as title companies and data resellers, to build and maintain private databases and perform a variety of queries.



Sources: GAO; Art Explosion (clip art)

Finding 1: Availability and use of records



## Some Businesses Rely on SSNs in Records More than Others

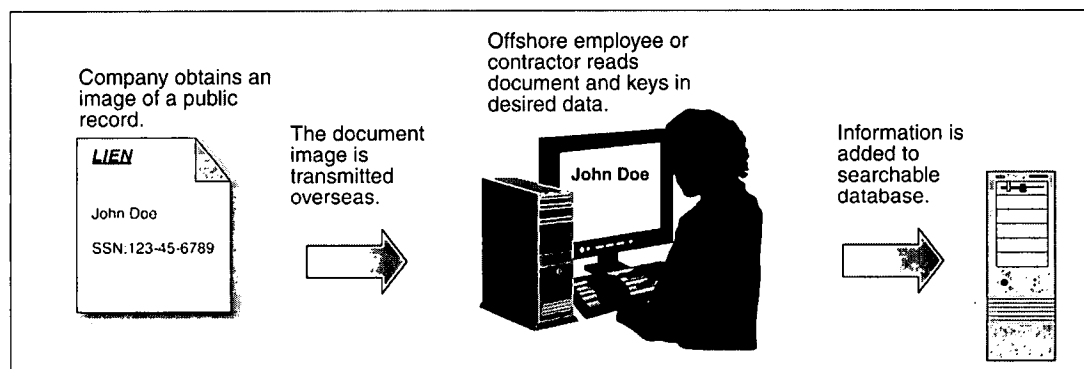
Some businesses told us...	Because...	Examples include...
Having the complete SSN is critical for them.	They must ensure that they match information to the correct individual. There are many people in the nation with the same name.	Consumer reporting agencies, people finders
A partial SSN (e.g., the last four digits) is sufficient.	They still need to match to an individual, but pertinent records are at the county level where the universe of individuals is smaller.	Title insurance industry <sup>2</sup>
Having an SSN is inconsequential.	They are not interested in matching data to individuals, but are instead interested in specific information such as recent home purchases.	Marketing firms

Source: GAO

<sup>2</sup> One title company told us that it is voluntarily truncating SSNs from the 4 billion documents in its repository.

## Some Businesses, Including the Title Industry, Send Document Images Overseas for Processing

- Officials from some companies we interviewed told us they share data from public records with offshore units or service providers
- India and the Philippines are two locations where public records data are sent.



Sources: GAO, Art Explosion (clip art)

### **Some Businesses, Including the Title Industry, Send Document Images Overseas for Processing (continued)**

- We were unable to determine the overall extent to which businesses send records containing SSNs overseas, but record keepers we interviewed believe it is common. Additionally, our survey shows that some offshore-based entities obtain records directly from counties.
- Several companies told us that they take measures to screen overseas employees and follow the same information security procedures in their overseas locations as they do in their U.S. locations.
- Additionally, companies told us they have various safeguards in place, including computer systems that restrict employees' access to records. The extent to which these protections are in place is unclear.

---

**Finding 2: Actions to protect SSNs in records**



**Some Counties Are Taking Actions to Remove SSNs from Public Records or Display Only Partial SSNs**

- Some counties have started redacting or truncating SSNs in publicly available versions of recorded documents, but are retaining full SSNs in nonpublic versions that are not available online or for bulk purchase.
- These actions have sometimes been taken in response to state laws: Several counties in California have begun planning for a new truncation requirement, and counties in Florida have begun redacting SSNs in existing records to comply with a state law.
- Other counties have taken the initiative to begin redaction on their own. For example, the county clerk in Travis County, Texas, began redacting SSNs in response to privacy concerns.

24

### **Some Counties Are Taking Actions to Remove SSNs from Public Records or Display Only Partial SSNs (continued)**

- On the basis of our survey, we estimate that about 12 percent of counties have redacted or truncated SSNs that appear in online or bulk records. Furthermore, another 26 percent are in the process of redacting or truncating SSNs.
- Large counties are more likely to be planning to redact or truncate SSNs in the future: 24 percent of large counties reported they plan to redact or truncate SSNs in the next two years, while less than 5 percent of smaller counties plan to do so.

## Some States Have Passed Laws to Limit the Availability of SSNs in Public Records

- In 2007, SSA's Office of Inspector General identified 25 states in a non-exhaustive search that have enacted some form of statutory limit on the display of SSNs in public records.<sup>3</sup> These include
  - 11 states that have taken steps to remove SSNs from public documents, unless SSNs are required by federal law to be included in those records.
  - 24 states that have passed laws to protect individuals SSNs from being on public documents.
  - Within these two groups, there is variation in the scope and applicability of these laws. For example:
    - Some states, such as New Jersey and Ohio, prohibit SSNs from appearing in any publicly recorded document.
    - Others limit the requirement to specific types of records; for example, Kansas and Utah prohibit SSNs from being shown in voter registration records.

<sup>3</sup> Office of the Inspector General, Social Security Administration, *State and Local Governments' Collection and Use of Social Security Numbers*, September 2007, A-08-07-17086. Additional information was obtained from the workpapers for this report. 26



## **Some States Have Passed Laws to Limit the Availability of SSNs in Public Records (continued)**

- We identified other state laws that allow individuals to request that their SSNs be removed from public records.
  - For example, Texas passed a law in 2007 allowing individuals to request that the first five digits of their SSNs be removed from specific public records.
  - Ohio and Tennessee permit veterans to request that their SSNs be redacted from their military discharge records.

## **States Have Begun to Enact Laws to Redact or Truncate SSNs Displayed in Public Records**

For example:

- California—Recorders must begin truncating SSNs in publicly available records recorded between 1980 and 2008. For records filed on or after January 1, 2009, recorders are required to truncate SSNs in the public versions of filings. They can petition their county board of supervisors for authority to charge additional fees.
- Florida—Since 2002, officials have been required to redact SSNs in records upon written request of the SSN holder, and parties filing documents have generally been required to exclude SSNs. SSNs in electronic records must be kept confidential beginning in 2011.
- Other states have narrower requirements—Virginia law authorizes circuit court clerks to redact SSNs from certain land records and provides that they may receive reimbursement for this effort from a state trust fund.

## Existing Federal Laws Do Not Address the Transfer of State and Local Public Records or the Display of SSNs in Them

- Major federal privacy and records laws we reviewed, including the Privacy Act and the Freedom of Information Act (FOIA), do not appear to restrict the bulk transfer of state or local public records or the display of SSNs in those records.
- A 1990 amendment to the Social Security Act requires that SSNs obtained or maintained pursuant to any provision of law enacted on or after October 1, 1990, be kept confidential.<sup>4</sup>
  - Officials at SSA and FTC staff were not aware of any actions taken to enforce this provision, and no regulations have been promulgated implementing the provision.<sup>5</sup>
  - We were unable to identify any federal or state cases addressing this provision, nor could we find anything relevant in the legislative history.
  - As a result, it is not clear whether or how this provision applies to state and local government sales of public records that may contain SSNs.

<sup>4</sup> 42 U.S.C. § 405(c)(2)(C)(viii).

<sup>5</sup> In their technical comments on a draft of this report, SSA officials noted that while SSA has general rulemaking authority with respect to this provision, it has not explored the extent of this authority. In addition, SSA officials stated that even if SSA were to promulgate regulations under this provision, it does not have the authority to enforce them. FTC does not have rulemaking authority under the amendment, according to FTC staff.

## Federal and Foreign Laws May Not Provide Protection for SSNs Sent Overseas

- We did not identify any federal law that provides protection for SSNs obtained from public records and sent to overseas locations by private parties that obtain public records in bulk or online.
- According to one study, no specific legislation pertaining to data protection has been enacted in India.<sup>6</sup> However, that study also noted that there may be other laws, such as the Information Technology Act of 2000, that address some issues related to data security.
- An offshore service provider based in the Philippines informed us its government has issued an administrative order enumerating guidelines for protecting personal data but it has not been enacted as law.

<sup>6</sup> CRID – University of Namur, *First Analysis of the Personal Data Protection Law in India: Final Report*, June 2005.

Finding 2: Actions to protect SSNs in records



## Selected Pending Federal Legislation Would Limit the Display or Sale of SSNs

<b>S. 238</b> Generally prohibits the display or purchase of SSNs without the express consent of the SSN holder; contains an exception for certain public records	<b>H.R. 948</b> Makes it unlawful for any person to sell or purchase SSNs in a manner violating regulations to be promulgated by SSA; does not have explicit provisions applicable to or exempting state and local governments
<b>S. 2915</b> Prohibits display of SSNs to the general public on the Internet by state and local governments unless truncation standards to be set by SSA in accordance with certain guidelines are met; considers certain unencrypted transmittals of SSNs through the Internet to be a public display	<b>H.R. 3046</b> With certain exceptions, restricts the sale and display of SSNs to the general public by government entities; Does not specifically address SSNs in public records; Requires SSA to develop uniform truncation standards

Source: GAO.

31

## Efforts to Limit Availability of Records with SSNs Are a Recent Development

- As we previously reported, IRS and DOJ are truncating SSNs in liens and other records that are filed with county record keepers.<sup>7</sup>
- County, state, and federal governments' efforts to limit availability of SSNs have increased in the last several years as concerns about the use of information in public records for identify theft grew.

<sup>7</sup> GAO, *Social Security Numbers: Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain*, GAO-07-752, (Washington, D.C., June 15, 2007).

## Concluding Observations

- Recent actions by states and counties to limit the display of SSNs in records made available to the public through redaction or truncation are positive steps. However, because millions of records with SSNs have already been obtained in bulk or online, these actions will protect SSNs only in future transfers.
- The bulk transfer of records raises other concerns about the security of SSNs because
  - Many record keepers do not or cannot restrict the types of entities that can obtain public records and may not know how records are being used.
  - Some businesses are sending records with SSNs offshore, even though not much is known about how they are protected overseas.

## Concluding Observations (continued)

- Any policy deliberations on further limiting the display of SSNs will need to consider and balance
  - the need to keep SSNs confidential and the longstanding tradition of open access to records,
  - the rights of states and localities to regulate the availability of their records, and
  - existing business practices and appropriate private sector use of SSNs.
- Recent actions by the IRS, the Department of Justice, and states to truncate SSNs represent one effort that may strike an appropriate balance between protecting SSNs from misuse and making a portion available to appropriate parties to firmly establish the identity of specific individuals.



---

---

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

---

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site ([www.gao.gov](http://www.gao.gov)). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to [www.gao.gov](http://www.gao.gov) and select "E-mail Updates."

---

## Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office  
441 G Street NW, Room LM  
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000  
TDD: (202) 512-2537  
Fax: (202) 512-6061

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)  
E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)  
Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Ralph Dawn, Managing Director, [dawnr@gao.gov](mailto:dawnr@gao.gov), (202) 512-4400  
U.S. Government Accountability Office, 441 G Street NW, Room 7125  
Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngcl@gao.gov](mailto:youngcl@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548

Appendix 2

*Security in Numbers: SSNs and ID Theft* (Federal Trade Commission  
Report, December 2008)

# Security in Numbers

\*\*\* - \*\* - \*\*\*\*

## SSNs and ID Theft

Federal Trade Commission Report  
December 2008

# RECOMMENDATIONS ON SOCIAL SECURITY NUMBER USE IN THE PRIVATE SECTOR

## I. Introduction

The President's Identity Theft Task Force ("Task Force") was established in May 2006 to develop a coordinated plan to prevent identity theft, help victims to recover, and prosecute the criminals who perpetrate it.<sup>1</sup> The Task Force issued its Strategic Plan, with 31 recommendations for action, in April 2007. One of those recommendations directed Task Force agencies to study the private sector uses of consumers' Social Security numbers ("SSNs"), develop a deeper understanding of the relationship between the SSN and identity theft, and explore approaches that would preserve the SSN's beneficial uses while curtailing its availability and value to identity thieves.<sup>2</sup>

This report answers the Task Force's mandate. Building on extensive fact-finding conducted by staff of the Federal Trade Commission ("FTC" or "Commission"), in cooperation with other Task Force agencies, the report examines the various private sector uses of the SSN and concludes with five specific FTC recommendations. These recommendations address both the supply and demand aspects of the SSN problem by proposing actions that would make SSNs less available to identity thieves, and would make it more difficult for them to misuse those SSNs they are able to obtain.

The Commission believes that the most effective course of action is to strengthen the methods by which businesses authenticate new and existing customers. Stronger authentication would make it more difficult for criminals to use stolen information, including SSNs, to impersonate consumers, thus devaluing the SSN to identity thieves and reducing the demand for it.

Limiting the supply of SSNs that are available to criminals, as a complement to improved authentication, although important, is more complex. SSNs already are available from many sources, including public records, and it may be impossible to "put the genie back in the bottle." Moreover, there is a danger that reducing the availability of SSNs would have unintended, adverse consequences. A number of important functions in our economy depend on access to SSNs. Businesses routinely rely on SSNs to ensure that the information they use or share with other organizations is matched to the right individual. Still, we believe it is feasible to reduce the availability of SSNs to identity thieves, such as by eliminating unnecessary public display, while preserving the legitimate and beneficial uses and transfers of SSNs. The Commission's five recommendations, detailed below in Section III, are:

- Improve consumer authentication;
- Restrict the public display and the transmission of SSNs;
- Establish national standards for data protection and breach notification;
- Conduct outreach to businesses and consumers; and
- Promote coordination and information sharing on use of SSNs.

## II. Background

The SSN was created in 1936 for the purpose of tracking workers' earnings for benefits purposes.<sup>3</sup> Since that time, however, SSN usage has expanded to encompass a myriad of purposes well beyond the operation of the Social Security system. Financial institutions, insurers, universities, health care entities, government agencies, and innumerable other organizations use this nine-digit sequence as a default identifier to ensure accurate matching of consumers with their information within organizations, to facilitate matching of consumer information with other organizations, and to avoid having to establish a different identification system for each set of benefits or records. Many SSN uses have also been legally mandated. The Internal Revenue Service ("IRS"), for example, requires private sector entities, including banks, insurance companies, and employers, to collect SSNs for income and tax-related purposes. The numerous uses of the SSN reflect its considerable advantages as an identifier, because it is permanent, ubiquitous, and unique to each individual.

Many entities also use SSNs to authenticate consumers, *i.e.*, to verify that individuals are who they say they are. These entities, in effect, treat the SSN as a secret piece of information, available only to the consumer and themselves, and give access to information or benefits only when the consumer is able to supply and confirm his or her SSN.

This dual use of the SSN as identifier and authenticator has created significant identity theft concerns. SSNs often are described as the "keys to the kingdom," because an identity thief with a consumer's SSN (and perhaps other identifying information) may be able to use that information to convince a business that he is who he purports to be, allowing him to open new accounts, access existing accounts, or obtain other benefits in the consumer's name. Unfortunately, SSNs have become increasingly available to identity thieves, at least in part because they are so widely used as identifiers. Identity theft continues to be a major problem in this country, with victims numbering in the millions each year and out-of-pocket losses (primarily to businesses) in the billions of dollars.<sup>4</sup>

In April 2007, the FTC hosted a public workshop on consumer authentication to examine, among other things, the utility and risks of using SSNs as authenticators.<sup>5</sup> Following the release of the Strategic Plan that same month, the Task Force agencies launched an extensive research and outreach effort to develop a comprehensive record on the uses of SSNs by the private sector. Staff from various Task Force agencies conducted outreach to more than fifty stakeholders. In addition, the FTC received more than 300 comments after it solicited public comment on the issue.<sup>6</sup>

In November 2007, the FTC staff published a summary of the comments and other information it compiled through the outreach effort, entitled *Staff Summary of Comments and Information Received Regarding the Private Sector's Use of Social Security Numbers* (hereinafter, "FTC Staff Summary").<sup>7</sup> The FTC Staff Summary includes an in-depth description of the ways in which the private sector uses and collects SSNs and the role SSNs play in identity theft. Subsequently, the FTC held a second public workshop in December of 2007, which focused specifically on steps that might be taken to make the SSN less available and valuable to identity thieves.<sup>8</sup>

This report presents the Commission's recommendations for actions to minimize the role that SSNs play in identity theft.

### **A. The Role of SSNs in Identity Theft**

As noted above, because private and public sector entities have used the SSN extensively as an identifier and in the authentication process, the SSN has become both available and valuable to identity thieves.<sup>9</sup> These criminals obtain the SSNs of the victims they impersonate and use them to facilitate the opening of new accounts, gain access to existing accounts, commit medical identity theft, seek employment, and obtain government benefits.<sup>10</sup> Although there is disagreement as to whether a thief can use the victim's name and SSN alone to steal her identity, it is generally understood that, at the least, the SSN facilitates identity theft, i.e., that it is a *necessary*, if not necessarily *sufficient*, data element for many forms of this crime to occur.<sup>11</sup>

Thieves gather SSNs in many ways, from the high-tech – e.g., hacking, phishing, malware, spyware, and keystroke loggers – to the low-tech – e.g., dumpster diving, stealing workplace records, stealing mail or wallets, and accessing public records containing SSNs.<sup>12</sup> What is not known, however, is the prevalence of each of these methods. This is due in large part to the fact that victims frequently do not know how their information was compromised.<sup>13</sup> Moreover, even if reliable prevalence data were available, it likely would become outdated quickly as identity thieves change techniques to harvest consumers' data.

A number of commenters also addressed another form of identity theft that does not depend on illegally acquired SSNs. Some thieves fabricate SSNs that either intentionally or coincidentally correspond to SSNs that already have been issued or are about to be issued. The thieves then use these SSNs – in conjunction with other information unrelated to the individuals to whom the SSNs actually correspond – to create new identities. This is commonly referred to as synthetic identity theft.<sup>14</sup> The existence of synthetic identity theft demonstrates that the solution to SSN-related identity theft will require more than simply eliminating the sources of existing SSNs for identity thieves.

### **B. The SSN as Identifier**

There appears to be broad consensus that the use of the SSN as an identifier – to match individuals to information about them both within an organization and between organizations – is prevalent and, in many contexts, beneficial.<sup>15</sup> Many organizations use SSNs as employee or customer identification numbers.<sup>16</sup> Some entities – including some insurers, universities, and government agencies – display the SSN on customer or employee identification cards, although this use is diminishing as noted below, while others use the SSN for data matching purposes “behind the scenes.” Entities also may use their customers' SSNs to ensure that the data they share about those customers with a myriad of third parties is that of the right person. These entities share data for many legitimate, beneficial, and (in some cases) legally required purposes, such as to report earnings information to the IRS,<sup>17</sup> share patient records within the health care system,<sup>18</sup> and access consumer reports.<sup>19</sup>

Many businesses contend that the SSN is superior to any other item of information currently available to identify consumers and link information to them. Commenters from various sectors of the economy asserted that there are no other identifiers that are as reliable, cost-effective, and accurate for data matching as SSNs, because only the SSN is permanent, unique, ubiquitous, and common

across organizations.<sup>20</sup> Moreover, many have observed that consumers find it convenient to have a single identifier that can be used across applications and organizations, rather than having to memorize multiple numbers.<sup>21</sup>

Recognizing identity theft concerns, some organizations that use SSNs to identify their customers or members no longer print them on identification cards or otherwise publicly display them. For example, an increasing number of insurers and universities have discontinued their use of SSNs as customer, subscriber, or student identification numbers, but may still use SSNs internally.<sup>22</sup> In addition, some entities have stopped using SSNs as internal identifiers within their organizations, although others have resisted doing so because the change-over to another identifier can be costly and time-consuming.<sup>23</sup>

### **C. SSNs and the Authentication Process**

"Authentication" is the process of verifying that someone is who he or she claims to be. It is distinguished from "identification," which simply matches an individual with his or her records, but does not prove that the individual is who he or she purports to be. Financial institutions, government agencies, and countless other organizations that enter into transactions with consumers authenticate individuals on a regular basis. It is when authentication fails – when an imposter successfully presents himself as someone else – that identity theft occurs. As the FTC Staff Summary noted, if authentication worked perfectly, identity thieves would not be able to use stolen consumer data to assume another's identity.<sup>24</sup>

Although there are many different kinds of authentication methods currently in use, they are not always adequate to prevent identity theft. According to the FTC Identity Theft Survey, 1.8 million consumers had new accounts opened fraudulently in their names in 2005, and another 6.5 million consumers experienced identity theft that involved exclusively existing bank account or credit account fraud.<sup>25</sup> These data suggest that identity thieves often are able to pass authentication screens successfully. There are different ways in which thieves might be doing so. Some thieves are able to obtain personal information about their victims beyond their SSNs that they then use to pass authentication tests. Others are able to obtain or manufacture fake drivers' licenses, similarly useful for authentication purposes. In other cases, businesses may not be requiring the right type of authentication (such as requiring only a name and SSN, or other readily available information, for account access), or their employees may not be following the company's procedures. The Commission knows of no reliable data showing the prevalence of the different methods by which criminals are passing authentication screening, but it is clear that they are able to do so in many instances.

As discussed above, there is a broad consensus that the use of the SSN as an identifier is often beneficial, but that its use as an authenticator – as proof of identity – is problematic. Identifiers are effective only when they are widely shared. One's name, for example, is widely known and generally effective as an identifier, although in many cases its lack of permanence or uniqueness prevents it from being useful as an identifier. Authenticators, on the other hand, are effective only when they are secret and thus not widely known. According to commenters and workshop participants, SSNs do not function well as authenticators because they are used commonly as identifiers and thus are widely available.<sup>26</sup>



Although the SSN generally is inadequate as a sole authenticator, it can be used effectively in the authentication *process*. Indeed, numerous organizations reported that they may ask a consumer to produce her SSN not because it is adequate authentication, but rather to link to other data sources that contain additional information about her that can be used to verify her identity. These data sources can take several forms. Some entities use the SSN to access databases containing information about an individual that can be used to formulate challenge questions that only the true individual should be able to answer (for example, the amount of her mortgage payment each month).<sup>27</sup> Other entities use the SSN to check an individual's identifying information against fraud databases (*i.e.*, databases with records of prior fraudulent transactions),<sup>28</sup> or as one element in their quantitative fraud prediction models, which are designed to flag suspect patterns of use of identifying information that might indicate that an application or proposed transaction is fraudulent.<sup>29</sup> These examples show that the SSN may not be well-suited as an authenticator itself, but can be and is used effectively to detect potential fraud by permitting access to other authentication-related information.<sup>30</sup>

### III. Recommended Approach for Addressing the Problem

The Commission believes that the most effective approach to the problem of SSNs and identity theft will be comprehensive and multi-faceted, designed to reduce both the supply of and demand for SSNs, and carefully tailored to avoid hindering unnecessarily the beneficial transfers and uses of SSNs.

When considering ways to minimize the role the SSN plays in identity theft, commenters and participants at the SSN workshop agreed that the beneficial uses of SSNs must be weighed carefully against the harms that result when they are misused by identity thieves.<sup>31</sup> While these individuals acknowledged that the problems associated with SSN use must be addressed, they also cautioned that certain approaches may create unintended, negative consequences.<sup>32</sup>

Given that the widespread use and availability of SSNs cannot be completely reversed,<sup>33</sup> the Commission believes that the central component of the solution is to reduce the demand for SSNs by minimizing their value to identity thieves. This could be achieved by encouraging or requiring entities that have consumer accounts that can be targeted by identity thieves to adopt more effective authentication procedures, thereby making it more difficult for wrongdoers to use SSNs to open new accounts, access existing accounts, or otherwise impersonate a consumer.<sup>34</sup>

In addition, because improved authentication is not a foolproof mechanism for stopping persistent and creative thieves, it remains important to take steps to limit the supply of SSNs to criminals as part of a comprehensive approach to the identity theft problem. Therefore, the Commission recommends that measures be taken to reduce the unnecessary display and transmission of SSNs and improve data security.

With respect to its central proposals – improving authentication, reducing unnecessary SSN display and transmission, improving data security, and requiring breach notification – the Commission recommends that Congress consider establishing national standards that would be delineated further through agency rulemaking. In addition, the Commission recommends that Congress consider granting it authority to obtain civil penalties for violations of these rules.

Finally, coordination and information sharing among entities that routinely use SSNs can help facilitate the dual goals of improving authentication and protecting SSNs.<sup>35</sup>

#### **A. Making It More Difficult to Use SSNs to Commit Identity Theft**

The first step in minimizing the role of SSNs in identity theft is to limit the demand for SSNs by making it more difficult for thieves to use them to open new accounts, access existing accounts, or obtain other benefits or services.

##### ***Recommendation 1: Improve Consumer Authentication***

Appropriate and reasonable authentication procedures can help prevent identity thieves from consummating their fraud. Although most financial institutions are subject to some authentication requirements promulgated by the bank regulatory agencies,<sup>36</sup> other businesses and organizations may not be subject to any such requirements. Requiring all private sector entities that maintain consumer accounts to establish appropriate, risk-based consumer authentication programs could reduce the misuse of consumer data and the prevalence of identity theft. Many workshop participants agreed that improving consumer authentication is critical.<sup>37</sup>

There have been some governmental efforts to extend authentication requirements beyond the financial sector. Some states have enacted laws that prohibit businesses from requiring consumers to use SSNs to log onto or access an Internet website, unless the SSNs are used in combination with a password or other authentication device.<sup>38</sup> One federal legislative proposal, H.R. 3046, calls for a study on the feasibility of banning the use of SSNs as authenticators.<sup>39</sup>

Generally speaking, however, private sector organizations outside the financial sector currently are not subject to any specific authentication requirements. Some workshop participants observed that such organizations may not have sufficient incentives to improve their authentication systems to an optimal level, because in many cases they are spared the full cost of identity theft.<sup>40</sup> Businesses certainly do suffer losses when identity thieves make fraudulent charges. Consumers themselves, however, often absorb some of the damage, including both direct losses and the time and emotional costs of recovery. Several workshop participants asserted that carefully-tailored government requirements may be necessary to set the proper incentives for improving authentication,<sup>41</sup> much as the Fair Credit Billing Act's limitation on cardholders' liability for disputed charges spurred the creation of a market for a variety of new fraud detection tools in the credit card industry.<sup>42</sup>

The Commission recommends that Congress consider establishing national consumer authentication standards covering all private sector entities that maintain consumer accounts other than financial institutions subject to the jurisdiction of the bank regulatory agencies, which already are subject to such requirements. These standards, which should be consistent with those covering financial institutions, should require private sector entities to create a written program that establishes reasonable procedures to authenticate new or existing customers. This "reasonable procedures" approach, which should be fleshed out through agency rulemaking, should be technology-neutral and provide flexibility to private sector entities to implement a program that is compatible with their size, the nature of their business, and the specific authentication risks they face. The procedures also

should be adaptable to changes that may occur over time in available technologies and the nature of the risks, including the potential harm to consumers. Finally, the standard should be one of reasonableness and not perfection, acknowledging that there is no fool-proof method of authenticating consumers and no likelihood that one will be developed in the foreseeable future.<sup>43</sup> "Reasonable procedures" requirements have been included in several recent identity theft-related rules promulgated by the FTC and the bank regulatory agencies pursuant to the Gramm-Leach-Bliley Act and the FACT Act.<sup>44</sup>

In developing authentication standards, Congress should consider several factors. First, the cost of implementing new authentication procedures should be evaluated in determining what is "reasonable." Second, consumer convenience is a critical concern and also should be weighed in the reasonableness determination. Consumers are likely to resist authentication requirements that are too time-consuming or difficult, or that require the memorization or retention of too much information. Third, more robust authentication procedures that require consumers to provide additional information about themselves raise potential privacy concerns. For instance, some businesses have developed authentication methods that require consumers to provide additional personal information either at the time the account is established or when the consumer later attempts to access the account. Many businesses use knowledge-based authentication in which they ask challenge questions, the answers to which are likely to be known only by the true individual. Although this method of authentication can overcome concerns about the unreliability of documentary evidence of identity<sup>45</sup> and the lack of personal interaction in telephone or online transactions, challenge questions may require consumers to provide increasing amounts of information to businesses that are linked together in ways that may be unsettling to some.<sup>46</sup>

Some commenters and workshop participants also suggested that, even in the absence of any national standards for authentication, the FTC could spur improved authentication by challenging inadequate authentication procedures, such as using an SSN as the sole authenticator, as unfair or deceptive practices prohibited by Section 5 of the Federal Trade Commission Act.<sup>47</sup> The Commission has challenged businesses that failed to provide reasonable security for sensitive consumer information as deceptive (when the business misrepresented its security practices)<sup>48</sup> or unfair (when the business's lack of reasonable security caused or was likely to cause substantial and unavoidable consumer injury).<sup>49</sup> Whether the failure to conduct reasonable authentication could constitute an unfair or deceptive practice would depend on the facts of a particular case, for example, whether the company made false or misleading claims or caused substantial consumer injury by its inadequate authentication. In appropriate cases, the Commission will consider law enforcement action against businesses that fail to maintain reasonable authentication procedures.<sup>50</sup>

## **B. Curtailing the Supply of SSNs to Wrongdoers**

Although decreasing the value of SSNs for identity thieves is essential to curbing their use in identity theft, limiting unnecessary SSN supply and availability remains important and would complement efforts to reduce SSN demand.

**Recommendation 2: Restrict the Public Display and the Transmission of SSNs**

Although SSNs are valuable as a means of linking consumers with their information, much can be done to reduce the availability of SSNs to identity thieves by eliminating the unnecessary display and transmission of SSNs by the private sector. Restricting the display of SSNs on publicly-available documents and identification cards, and limiting the circumstances and means by which they can be transmitted, would make it more difficult for thieves to obtain SSNs, without hindering their use for legitimate identification and data matching purposes.<sup>51</sup>

Many organizations already have discontinued using SSNs as employee or customer numbers, or have stopped printing them on identification cards or in mailings to customers.<sup>52</sup> Yet, some businesses, universities, and other private sector entities still include SSNs on identification cards, thereby exposing them in the event that an individual's wallet is lost or stolen.<sup>53</sup> Moreover, some organizations continue to display SSNs on account statements, paychecks, applications, or other documents that are sent through the mail, which puts consumers at risk for identity theft if their mail is stolen or if the documents are thrown in the trash without being shredded.<sup>54</sup> SSNs also can be exposed to potential identity thieves by inadvertent display, including on websites.<sup>55</sup>

Some states have enacted laws limiting the display and/or transmission of SSNs.<sup>56</sup> California was the first state to pass such a law, which prohibits the printing of SSNs on identification and membership cards and certain documents mailed to customers and bars the emailing of unencrypted SSNs.<sup>57</sup> Several other states have followed California's lead.<sup>58</sup> Workshop participants and commenters generally reported that provisions of state laws that restrict public display are not unduly burdensome.<sup>59</sup> They asserted that the process of removing SSNs from identification cards and public documents generally is easier than eliminating the use of SSNs for internal or external data matching, which can create inefficiencies and be expensive.<sup>60</sup>

Some workshop participants and commenters asserted that switching from the display of full SSNs to truncated SSNs could help reduce identity theft.<sup>61</sup> These observers note that partial SSNs still can be useful in identifying and authenticating consumers, although not to the extent of full SSNs.

It is true that truncated SSNs generally are less valuable to identity thieves than full SSNs, because many entities will not allow customers to open or access accounts without a full SSN. There are some situations, however, in which a thief could use a truncated SSN to steal an identity. First, some organizations may accept truncated SSNs as adequate authentication, at least in certain instances such as when a customer wishes to access his account via telephone or online. Second, inconsistencies in the means by which entities truncate could create an opening for an identity thief to obtain a full SSN. Currently, there are varying conventions for SSN truncation – some entities, for example, block the first five digits while others block the last four digits.<sup>62</sup> Thus, an identity thief could piece together the full SSN by obtaining different parts of the number from different sources. Third, because the Social Security Administration uses date and location of issuance to determine the first five digits of the SSN, some observers have posited that identity thieves could use a truncated SSN, augmented by other personal information that they obtain and some guess work, to determine the full SSN.<sup>63</sup>

The Commission recommends that Congress consider creating national standards for the public display and the transmission of SSNs.<sup>64</sup> Federal legislation would establish a nationwide approach to

reducing unnecessary display and transmission of SSNs, while addressing concerns about a patchwork of state laws with varying requirements. National standards should prohibit private sector entities from unnecessarily exposing SSNs. The precise standards should be developed in rulemaking by appropriate federal agencies (*i.e.*, agencies that oversee organizations that routinely transmit or display SSNs), and should include, for example, prohibitions against:

- publicly posting or displaying SSNs;
- placing SSNs on cards or documents required for an individual to access products or services provided by a covered entity, including student ID cards, employee ID cards, and insurance cards;
- transmitting (or requiring an individual to transmit) an SSN over the Internet, unless the connection is secure from unauthorized access, *e.g.*, by encryption or other technologies that render the data generally unreadable;
- printing an individual's SSN in materials mailed to the individual; and
- printing an individual's SSN on the outside of an envelope or other mailer, or in a location that is visible without opening the envelope or mailer.

Any such standards should allow for the display and transmission of SSNs when required by law and in specified circumstances where there is a substantial business need that outweighs the risks of exposure. For example, California has created exceptions for SSNs that are included in forms mailed as part of an enrollment process and for documents necessary to establish an account or contract, provided that the SSN is not visible without opening the transmitting envelope.<sup>65</sup> Federal agency rulemaking should similarly evaluate acceptable circumstances for display and transmission. In addition, the standards should take into account the benefits and risks of allowing the display and transmission of truncated SSNs. Finally, entities should be given a sufficient phase-in period for implementation, given the often significant cost of modifying systems to avoid displaying SSNs.

***Recommendation 3: Establish National Standards for Data Protection and Breach Notification***

An important step in limiting the supply of SSNs is for entities that collect and store sensitive consumer information to safeguard it against unauthorized access. Safeguards requirements currently exist with respect to certain industries, certain types of data, and in certain states. The Safeguards Rules promulgated by the FTC and the federal banking agencies pursuant to the Gramm-Leach-Bliley Act, for example, require financial institutions to establish reasonable procedures to protect consumers' personally identifiable financial information, which may include SSNs.<sup>66</sup> Many entities or types of data are not subject to federal data security standards, however. The Commission has previously expressed support for national data security standards that would cover SSNs in the possession of any private sector entity,<sup>67</sup> and numerous commenters and workshop participants voiced similar support.<sup>68</sup> Such standards, which would be implemented in rulemaking by federal agencies that oversee entities that routinely use and transfer sensitive consumer information, could be modeled after the Safeguards Rules and cover all entities that maintain sensitive consumer information.

The Commission also reiterates its support of its prior recommendation that Congress consider establishing national data breach notification standards requiring private sector entities to provide public notice when the entity suffers a breach of consumers' personal information and the breach creates a significant risk of identity theft or other harms.<sup>69</sup> These standards would also be implemented in rulemaking by appropriate federal agencies. Most states now have breach notification laws,<sup>70</sup> but currently there is no across-the-board federal requirement.<sup>71</sup> Commenters and workshop participants noted that, in addition to alerting affected consumers to protect themselves, these laws have had the indirect benefit of motivating companies to weigh their need to collect SSNs against the potential cost and liability that may ensue if the SSNs are compromised.<sup>72</sup> Participants also noted that many businesses have strengthened their safeguards practices to avoid data breaches, at least in part as a result of breach notification requirements.<sup>73</sup> The state laws differ in various respects, however, complicating compliance.<sup>74</sup>

#### ***Recommendation 4: Conduct Outreach to Businesses and Consumers***

The Commission recommends increasing education and guidance efforts as additional steps to help reduce the role of SSNs in facilitating identity theft. Over the past several years, the Commission and other Task Force agencies (including the Social Security Administration, the Department of Health and Human Services, and the U.S. Postal Inspection Service) have conducted extensive outreach, both to businesses and consumers, on identity theft prevention and recovery, data protection, and safe computing. Many of the published materials discuss SSNs specifically, with advice to consumers on protecting their SSNs from wrongdoers.<sup>75</sup>

The Commission anticipates disseminating additional guidance to businesses on what they can do to reduce their use of SSNs and to safeguard SSNs when they are used. This guidance would ultimately include information regarding any national standards Congress creates for authentication, SSN display and transmission, data protection, and breach notification. This type of guidance would be especially useful to small businesses and could include the following messages:

- the importance of collecting SSNs only when necessary and storing them only as long as necessary;
- steps businesses can take to reduce the use of SSNs as internal identifiers;
- proper disposal of SSNs;
- the importance of securing SSNs (such as by encrypting them) during their transmission; and
- limiting employee access to SSNs and conducting employee screening and training.

The Commission also anticipates issuing additional guidance to consumers directed specifically at how they can protect their SSNs. This guidance will explain the various ways identity thieves obtain SSNs, from phishing to wallet theft, and how consumers can best protect their personal information. It also will address safe disposal practices and the questions consumers should ask when a business requests their SSN. Continuing and augmenting these education efforts will help maximize consumer awareness of risks and lead to decreased exposure to identity theft.

### C. Improving Coordination and Information Sharing

#### ***Recommendation 5: Promote Coordination and Information Sharing on Use of SSNs***

Many private sector entities, from large multi-nationals and universities to small businesses and health care systems, have described the difficulties and expense of removing SSNs from computer systems and files, as well as the challenges of keeping up with the sophisticated and changing methods of identity thieves.<sup>76</sup> Coordination and information sharing among private sector entities and between government and the private sector could assist entities in finding ways to reduce their uses of and better protect SSNs and improve their authentication processes. The Commission recommends that appropriate governmental entities explore helping private sector organizations establish a clearinghouse of best practices, enabling those organizations to share approaches and technologies on SSN usage and protection, fraud prevention, and consumer authentication.

## **IV. Conclusion**

Since the creation of the SSN in 1936, the private sector increasingly has utilized it for various purposes – both as an identifier and an authenticator – because it is the only permanent, unique piece of information that most Americans have about themselves. The SSN's use has expanded as organizations have adapted their business and record-keeping systems to utilize increasingly sophisticated automated data processing. The SSN has, over time, become an integral part of our financial system.

As the private sector's use of the SSN has grown, so too has its availability and value for identity thieves. The Commission believes that a number of actions could be taken to reduce the role of SSNs in identity theft, with emphasis on reducing the demand for SSNs by minimizing their value to identity thieves through improved authentication processes. Most importantly, the Commission recommends that Congress consider establishing national authentication standards for businesses that have consumer accounts and are not already subject to authentication requirements from other federal agencies.

Because authentication can never be perfect, however, the Commission also recommends carefully targeted actions to limit the supply or availability of SSNs to identity thieves. Specifically, the Commission recommends that Congress consider prohibiting the display of SSNs on publicly-available documents, identification cards, and other materials that could potentially fall into the hands of identity thieves. The Commission also recommends that Congress set national safeguards and breach notification standards, because better-protected SSNs are less likely to fall into the hands of criminals. Finally, the Commission is committed to educating consumers on protecting their SSNs and businesses on reducing their use of SSNs, and recommends that the government and private sector entities explore information sharing and other cooperative efforts to achieve these goals.

Together, these actions could substantially reduce the misuse of SSNs by identity thieves, while at the same time preserving the beneficial uses of SSNs in our economic system.

## Endnotes

- 1 The Task Force is comprised of 17 federal agencies and is co-chaired by the Attorney General and the Chairman of the Federal Trade Commission. See Exec. Order No. 13,402, 71 Fed. Reg. 27,945 (May 10, 2006).
- 2 See The President's Identity Theft Task Force, *Combating Identity Theft, A Strategic Plan* (April 2007), available at <http://www.idtheft.gov/reports/StrategicPlan.pdf> (hereinafter "Strategic Plan"). The Task Force also made a number of recommendations regarding the public sector's use of SSNs, highlighting the importance of limiting unnecessary use of SSNs by federal departments and agencies. See *id.* at 23-27. Many of these recommendations regarding limiting use and display of SSNs have been implemented. The status of these recommendations is described in the recent *Identity Theft Task Force Report*. See President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), at 6-8 and 51, available at <http://www.ftc.gov/os/2008/10/081021taskforcereport.pdf>.
- 3 Social Security Online, Social Security Number Chronology, <http://www.ssa.gov/history/ssn/ssnchron.html>.
- 4 Federal Trade Commission – 2006 Identity Theft Survey Report 3 & 9 (Nov. 2007), available at <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf> (hereinafter "FTC Identity Theft Survey").
- 5 Proof Positive: New Directions for ID Authentication, <http://www.ftc.gov/bcp/workshops/proofpositive/index.shtml>.
- 6 These public comments are available at <http://www.ftc.gov/os/comments/ssnprivatesector/index.shtm>.
- 7 Staff Summary of Comments and Information Received Regarding the Private Sector's Use of Social Security Numbers (Nov. 2007), available at <http://www.ftc.gov/bcp/workshops/ssn/staffsummary.pdf> (hereinafter "FTC Staff Summary").
- 8 Security in Numbers: SSNs and Identity Theft, <http://www.ftc.gov/bcp/workshops/ssn/index.shtm>.
- 9 Transcript of Security in Numbers: SSNs and ID Theft Workshop (Dec. 10, 2007) at 184-85, (hereinafter "Transcript of SSN Workshop"), Remarks of Dr. Annie I. Anton, Associate Professor, North Carolina State University, and Director, PrivacyPlace.org (explaining that the use of the SSN for both identification and authentication makes it more valuable to an identity thief).
- 10 See, e.g., FTC Staff Summary, at 14-18; Transcript of SSN Workshop (Dec. 10, 2007) at 62-63, Remarks of John K. Webb, Assistant U.S. Attorney, Southern District of West Virginia (discussing various ways SSNs are used to commit identity theft, including hijacking existing accounts and opening new accounts).
- 11 Some commenters and workshop participants asserted that identity thieves need additional information beyond a consumer's name and SSN to open a new account, while others argued the opposite, noting instances in which credit was granted based on applications full of inconsistencies and mismatched information. See FTC Staff Summary, at 14, 17. The FTC's latest survey found that approximately 1.8 million instances of new account identity theft occurred in 2005, the vast majority of which presumably involved the misuse of the victim's SSN. See FTC Identity Theft Survey, at 3. What the data do not reveal, however, is what additional information, if any, the thieves had that enabled them to open the accounts.



- 12 See, e.g., FTC Staff Summary, at 9-14; Transcript of SSN Workshop (Dec. 10, 2007) at 26-29, Remarks of John K. Webb, Assistant U.S. Attorney, Southern District of West Virginia (discussing numerous ways identity thieves obtain SSNs, including hacking, phishing, and stealing mail or wallets).
- 13 The FTC's Identity Theft Survey found that 56% of the identity theft victims surveyed did not know how their personal information was obtained. See FTC Identity Theft Survey, at 30. Similarly, the 2007 Identity Fraud Survey by Javelin Strategy and Research found that 58% of identity theft victims did not know how their personal information was obtained. Javelin Strategy and Research, *2007 Identity Fraud Survey Report: Identity Fraud Is Dropping, Continued Vigilance Necessary* 30 (Feb. 2007). Needless to say, successful thieves are unlikely to reveal their "tools of the trade."
- 14 See FTC Staff Summary, at 16-17.
- 15 These basic concepts are discussed in greater detail in the FTC Staff Summary.
- 16 See, e.g., FTC Staff Summary, at 19-20.
- 17 See, e.g., Transcript of SSN Workshop (Dec. 10, 2007) at 149-153, Remarks of Valerie Abend, Deputy Assistant Secretary for Critical Infrastructure Protection and Compliance Policy, U.S. Department of the Treasury (explaining the various ways the Treasury Department requires the private sector to collect and report SSNs).
- 18 See, e.g., FTC Staff Summary, at 22; Transcript of SSN Workshop (Dec. 10, 2007) at 168, Remarks of Roberta B. Meyer, Vice President and Associate General Counsel, American Council of Life Insurers (explaining that many healthcare providers are concerned about disclosing health records without being provided an SSN).
- 19 See, e.g., FTC Staff Summary, at 21-22; Transcript of SSN Workshop (Dec. 10, 2007) at 156-161, Remarks of Robert F. Ryan, Vice President for Government Affairs, TransUnion (describing the various ways the consumer reporting industry utilizes SSNs).
- 20 See, e.g., FTC Staff Summary, at 19-26; Transcript of SSN Workshop (Dec. 10, 2007) at 165, Remarks of Roberta B. Meyer, Vice President and Associate General Counsel, American Council of Life Insurers (explaining that the SSN is an important identifier because it is unique and does not change over time); Transcript of SSN Workshop (Dec. 10, 2007) at 102, Remarks of Jim Davis, Associate Vice Chancellor for Information Technology & CIO, University of California-Los Angeles (noting the importance of the SSN as an identifier because it typically does not change); Transcript of SSN Workshop, (Dec. 10, 2007) at 175, 179-180, Remarks of Michael C. Lamb, Vice President and General Counsel, LexisNexis Risk and Information Analytics Group (stating that the SSN is the one data point that persists and is unique and that SSN use for data linking "is extremely important"); Transcript of SSN Workshop (Dec. 10, 2007) at 156, Remarks of Robert F. Ryan, Vice President for Government Affairs, TransUnion (noting that the SSN helps ensure that credit files are accurate and complete).
- 21 See, e.g., Transcript of SSN Workshop (Dec. 10, 2007) at 39, Remarks of Lael Bellamy, Director-Legal, The Home Depot (discussing the convenience of accessing a consumer's credit account simply by punching the SSN into a key pad); Transcript of SSN Workshop (Dec. 10, 2007) at 120-21, Remarks

- of Kimberly Gray, Chief Privacy Officer for Highmark, Inc. (noting that customers often ask to use their SSN for authentication purposes because they find it convenient).
- 22 See, e.g., FTC Staff Summary, at 23-24; Transcript of SSN Workshop (Dec. 10, 2007) at 89-93, Remarks of Kimberly Gray, Chief Privacy Officer for Highmark, Inc. (describing process of removing SSNs from insurance identification cards); Transcript of SSN Workshop (Dec. 10, 2007) at 96, Remarks of Jim Davis, Associate Vice Chancellor for Information Technology & CIO, University of California-Los Angeles (describing process of removing SSNs from university identification cards).
- 23 See, e.g., FTC Staff Summary, at 24; Transcript of SSN Workshop (Dec. 10, 2007) at 40-41, Remarks of Lael Bellamy, Director-Legal, The Home Depot (noting that project to remove unnecessary SSNs at The Home Depot took approximately two years).
- 24 FTC Staff Summary, at 26.
- 25 FTC Identity Theft Survey, at 3.
- 26 See, e.g., FTC Staff Summary, at 26-27; Transcript of SSN Workshop (Dec. 10, 2007) at 184-85, Remarks of Dr. Annie I. Anton, Associate Professor, North Carolina State University, and Director of the PrivacyPlace.org (noting that use of the SSN as both an identifier and authenticator is problematic).
- 27 See, e.g., FTC Staff Summary, at 29; Transcript of SSN Workshop (Dec. 10, 2007) at 162-63, Remarks of Stan Szwalbenest, Remote Channel Risk Director, JPMorgan Chase Consumer and Retail Franchise (describing the process of using SSNs to obtain knowledge-based authentication questions from consumer reporting agencies).
- 28 See, e.g., FTC Staff Summary, at 30.
- 29 See, e.g., FTC Staff Summary, at 30-31; Transcript of SSN Workshop (Dec. 10, 2007) at 240-45, Remarks of Thomas Oscherwitz, Vice President of Government Affairs and Chief Privacy Officer, ID Analytics (describing how ID Analytics uses the SSN in its quantitative fraud prediction model).
- 30 See, e.g., FTC Staff Summary, at 26-31; Transcript of SSN Workshop (Dec. 10, 2007) at 237, 240, Remarks of Jennifer Barrett, Global Privacy Officer, Acxiom Corporation (stating that without use of the SSN, Acxiom's ability to validate an individual's information would decrease significantly, and noting that she does not know of an equivalent substitute for the SSN for linking data for authentication).
- 31 See FTC Staff Summary, at 19-26, 43; *see also* Strategic Plan, at 26-27.
- 32 See, e.g., Transcript of SSN Workshop (Dec. 11, 2007) at 59, Remarks of Jim McCartney (noting the inevitability of unintended consequences from making changes to SSN usage); Transcript of SSN Workshop (Dec. 11, 2007) at 95, Remarks of Fred Cate, Distinguished Professor and Director for Applied Cybersecurity Research, Indiana University, and Senior Policy Advisor, Center for Information Policy Leadership, Hunton & Williams (commenting on the potential for increased fraud if access to data useful for fraud detection purposes is restricted; also noting the potential for increased consumer inconvenience if data uses are restricted); FTC Staff Summary, at 31-32 (reviewing commenters' concerns that restrictions on SSN usage would make fraud detection and employee and volunteer screening more difficult).
- 33 Many workshop participants and commenters noted that SSNs already are widely available, and any attempt now to "put the genie back in the bottle" likely would be of limited value. Transcript of SSN

Workshop (Dec. 10, 2007) at 254-55 and Transcript of SSN Workshop (Dec. 11, 2007) at 126-27, Remarks of Tom Oscherwitz, Vice President of Government Affairs and Chief Privacy Officer, ID Analytics; Transcript of SSN Workshop (Dec. 11, 2007) at 155, Remarks of Fred Cate, Distinguished Professor and Director for Applied Cybersecurity Research, Indiana University, and Senior Policy Advisor, Center for Information Policy Leadership, Hunton & Williams.

- 34 Some suggested approaches to the problem of SSNs and identity theft focus on restricting the sale or transfer of SSNs to prevent thieves from obtaining them in the first instance, rather than reducing the value of SSNs to identity thieves once obtained. See FTC Staff Summary, at 38-39. These approaches also seek to preserve beneficial uses of SSNs. For example, some proposals would allow specified beneficial transfers (e.g., for credit reporting or fraud prevention purposes), and some would authorize the FTC or other agencies to create additional exemptions. The Commission believes that it would be extremely difficult, however, to craft the exemptions with sufficient precision so as to eliminate harmful transfers while permitting beneficial ones. If drafted too broadly, the exemptions could “swallow” the rule, so that virtually any type of transfer could fit within one or more exemptions. See generally Transcript of SSN Workshop (Dec. 11, 2007) at 156, Remarks of James Lewis, Senior Fellow and Director of the Technology and Public Policy Program, Center for Strategic and International Studies. Conversely, if the exemptions were drafted too narrowly, the rules could inadvertently prohibit beneficial transfers. Further complicating this task is the fact that some transfers of SSNs could serve both a beneficial purpose and raise risks of harm. For example, SSNs often are used for locating individuals, which could be for beneficial purposes (e.g., finding witnesses or beneficiaries), or harmful purposes (e.g., stalking).
- 35 This report focuses on recommendations to minimize the role of SSNs in identity theft, and does not address whether additional criminal penalties related to other types of misuse of SSNs are appropriate. For example, there have been reports of stalkers and other criminals obtaining and using SSNs to locate their victims. *Protecting the Social Security Number from Identity Theft: Hearing Before the Subcomm. on Social Security of the H. Comm. on Ways and Means*, 110th Cong. (June 21, 2007) (statement of Rep. Ed Markey).
- 36 For example, the guidance on authentication released by the Federal Financial Institutions Examination Council (“FFIEC”) advises companies of the risk management controls they should adopt to authenticate the identity of customers in the electronic banking context. See FFIEC, *Authentication in an Internet Banking Environment*, available at [http://www.ffiec.gov/pdf/authentication\\_guidance.pdf](http://www.ffiec.gov/pdf/authentication_guidance.pdf). In addition, the Customer Identification Program (“CIP”) rule, promulgated by the federal banking agencies (the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation) and the National Credit Union Administration (“NCUA”) under the USA PATRIOT Act, although not designed to prevent identity theft, mandates that, before opening a new consumer account, a financial institution or other covered entity must “form a reasonable belief that it knows the true identity of each customer.” 31 C.F.R. §§ 103.121(b)(2), 103.122(b)(2), 103.123(b)(2) & 103.131(b)(2). Finally, the Identity Theft Red Flags rules, recently promulgated by the FTC, the federal banking agencies, and the NCUA pursuant to the FACT Act of 2003, require most financial institutions and creditors to develop and implement an Identity Theft Prevention Program that includes reasonable policies and procedures for detecting, preventing, and mitigating identity theft in connection with existing accounts or the opening of new accounts. 16 C.F.R. § 681.2. These procedures may include enhanced customer authentication.

- 37 For example, workshop participants highlighted the importance of avoiding the use of the SSN as the sole authenticator. See Transcript of SSN Workshop (Dec. 10, 2007) at 185, Remarks of Dr. Annie I. Anton, Associate Professor, North Carolina State University, and Director, PrivacyPlace.org; Transcript of SSN Workshop (Dec. 10, 2007) at 218, Remarks of Beth Givens, Director, Privacy Rights Clearinghouse; Transcript of SSN Workshop (Dec. 10, 2007) at 254 and (Dec. 11, 2007) at 127, Remarks of Tom Oscherwitz, Vice President of Government Affairs and Chief Privacy Officer, ID Analytics; Transcript of SSN Workshop (Dec. 11, 2007) at 93-94, 155, Remarks of Fred Cate, Distinguished Professor and Director for Applied Cybersecurity Research, Indiana University, and Senior Policy Advisor, Center for Information Policy Leadership, Hunton & Williams; Transcript of SSN Workshop (Dec. 11, 2007) at 131, Remarks of James Lewis, Senior Fellow and Director of the Technology and Public Policy Program, Center for Strategic and International Studies; Transcript of SSN Workshop (Dec. 11, 2007) at 25, Remarks of Stuart Pratt, President and CEO, Consumer Data Industry Association; Transcript of SSN Workshop (Dec. 11, 2007) at 46, Remarks of Bob Blakley, Principal Analyst, Burton Group; Transcript of SSN Workshop (Dec. 11, 2007) at 154-55, Remarks of Chris Jay Hoofnagle, Senior Staff Attorney, Samuelson Law, Technology and Public Policy Clinic, UC Berkeley School of Law.
- 38 See, e.g., Tenn. Code Ann. § 47-18-2110 (2008).
- 39 Social Security Number Privacy and Identity Theft Protection Act of 2007, H.R. 3046, 110th Cong. § 14 (2007).
- 40 See Transcript of SSN Workshop (Dec. 11, 2007) at 33, Remarks of Jeanine Kenney, Senior Policy Analyst, Consumers Union; Transcript of SSN Workshop (Dec. 11, 2007) at 19-20, Remarks of Bob Blakley, Principal Analyst, Burton Group.
- 41 See Transcript of SSN Workshop (Dec. 11, 2007) at 46-47, Remarks of Bob Blakley, Principal Analyst, Burton Group; Transcript of SSN Workshop (Dec. 11, 2007) at 107-108, Remarks of James Lewis, Senior Fellow and Director of the Technology and Public Policy Program, Center for Strategic and International Studies.
- 42 15 U.S.C. § 1666-1666j. Workshop participants discussed a number of innovative authentication techniques or programs, such as the use of third-party identity providers. To date, these innovations have not flourished for reasons that may include the lack of market incentives. See Transcript of Proof Positive: New Directions in ID Authentication Workshop (Apr. 23-24, 2007), Panel 7, at 26-27, (hereinafter "Transcript of Authentication Workshop"), Remarks of Fred Schneider, Professor, Computer Science Department, Cornell University (explaining that regulations may be needed to "fix the market" and create incentives for better authentication); Transcript of SSN Workshop (Dec. 11, 2007) at 19-21, Remarks of Bob Blakley, Principal Analyst, Burton Group (stating that externalities could be addressed by third-party identity providers, or "identity oracles"). Workshop participants also noted the importance of consumer convenience in any authentication system. See Transcript of Authentication Workshop, Panel 5, at 11, Remarks of Cynthia Bohman, Manager, Cyber Fraud Risk, Discover Financial Services (discussing the importance of consumer convenience to an authentication system). Creating appropriate incentives is likely to encourage the development of authentication techniques that are both effective and convenient.
- 43 In some cases, even using multiple authenticators will not prevent identity theft, if the thief has sufficient information about his victim. Some organizations match identifying information provided by an applicant to that found in a third-party database, such as that of a consumer reporting agency, but this

process only detects mismatched information and would not detect an identity thief who has provided sufficient, accurate identifying information. Other companies may rely on checking a driver's license to authenticate an individual, but identity thieves can obtain falsified licenses. FTC Staff Summary, at 27.

- 44 These include: (1) the Safeguards Rules, which require financial institutions to have a written data security program with reasonable procedures to identify and address risks to customers' personally identifiable financial information, 16 C.F.R. Part 314; (2) the Disposal Rules, which require that businesses implement reasonable procedures to ensure that certain sensitive information is disposed of in a safe manner, 16 C.F.R. Part 682; and (3) the Identity Theft Red Flags Rules, which require most financial institutions and creditors to develop and implement a written Identity Theft Prevention Program that includes reasonable policies and procedures for detecting, preventing, and mitigating identity theft in connection with existing accounts or the opening of new accounts, 16 C.F.R. Part 681.
- 45 Participants at both the authentication and SSN workshops noted that documents frequently used for authentication when creating an account, such as driver's licenses, Social Security cards, and birth certificates, can easily be forged. See Transcript of Authentication Workshop, Panel 3, at 2-4, Remarks of Garland Land, Executive Director, National Association for Public Health Statistics and Information Systems (explaining weaknesses in birth certificate issuance process); Transcript of Authentication Workshop, Panel 3, at 19, Remarks of Ari Schwartz, Deputy Director, Center for Democracy and Technology (discussing the need for strengthening the driver's license issuance process); Transcript of SSN Workshop (Dec. 10, 2007) at 26, Remarks of John K. Webb, Assistant United States Attorney, Southern District of West Virginia (addressing ease of forging SSN cards).
- 46 See Transcript of SSN Workshop (Dec. 11, 2007) at 49, Remarks of Stuart Pratt, President and CEO, Consumer Data Industry Association. In some cases, challenge questions may be based on information the business already has or is able to obtain from outside data sources, *e.g.*, what financial institution holds the consumer's mortgage. See Transcript of Authentication Workshop, Panel 4, at 14-16, 19, Remarks of Micheline Casey, Senior Director, Identity Management, Choicepoint Government Services (explaining the process used to create knowledge-based authentication questions). In other cases, businesses may ask the consumer to establish questions and answers at the time of account enrollment, known as shared secrets, to be used for subsequent account access. Such questions and answers may be about a customer's pets, previous vehicles owned, family members, etc. See Transcript of Authentication Workshop, Panel 7, at 29, Remarks of Thomas Oscherwitz, Chief Privacy Officer, ID Analytics (noting that in an environment where information is available, for example, through social networking sites, shared secrets must become more and more personal in order to defeat the fraudsters). In either event, the business is compiling and maintaining additional information about the consumer. Because there currently are no broad-based restrictions on using this information for other purposes, or sharing it with third parties, some participants at the authentication workshop suggested that the government should enact broader privacy rules so that consumers will willingly participate in systems requiring stronger authentication. See Transcript of Authentication Workshop, Panel 7, at 4, Remarks of James Lewis, Senior Fellow and Director of the Technology and Public Policy Program, Center for Strategic and International Studies; Transcript of Authentication Workshop, Panel 7, at 27, Remarks of Jeffrey Friedberg, Chief Privacy Architect, Microsoft (discussing privacy concerns raised by authentication technologies that allow the linking of personal data).
- 47 See, *e.g.*, Transcript of SSN Workshop (Dec. 11, 2007) at 88-89, Remarks of Chris Jay Hoofnagle, Senior Staff Attorney, Samuelson Law, Technology and Public Policy Clinic, UC Berkeley School of Law; Comment of Center for Information Policy Leadership at Hunton & Williams, at 5. A deceptive

practice, pursuant to 15 U.S.C. § 45, "is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment." FTC Policy Statement on Deception, Oct. 14, 1983, available at <http://www.ftc.gov/bcp/policystmt/ad-decept.htm>. An unfair practice is an "act or practice [that] causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n).

- 48 *United States v. ValueClick, Inc.*, No. CV08-01711 (C.D. Cal. Mar. 13, 2008); *In the Matter of Goal Financial, LLC*, FTC Docket No. C-4216 (April 15, 2008); *In the Matter of Life is Good, Inc.*, FTC Docket No. C-4218 (Apr. 18, 2008); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Apr. 3, 2007); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); and *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002).
- 49 *In the Matter of The TJX Companies*, FTC Docket No. C-4227 (Aug. 1, 2008); *In the Matter of Reed Elsevier Inc. and Seisint Inc.*, FTC Docket No. C-4226 (Aug. 1, 2008); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006); *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); and *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002).
- 50 Inadequate authentication could violate other existing laws or regulations as well. The Safeguards Rules, for example, require financial institutions to maintain reasonable protections for personally identifiable financial information, which could include SSNs. The duty to protect this information could include, in appropriate cases, the duty to employ reasonable authentication procedures to prevent unauthorized persons from gaining access to consumers' accounts and records. Similarly, the Identity Theft Red Flags Rules require covered entities to detect signs of identity theft, which might be addressed by improving authentication procedures for both account opening and account access requests. See 16 C.F.R. § 681.2.
- 51 See FTC Staff Summary, at 23 ("Not displaying SSNs on cards, which are frequently carried by the holder, decreases the risk of identity theft through loss, theft, or duplication of the card."); Transcript of SSN Workshop (Dec. 10, 2007) at 107, Remarks of Kim Duncan, Vice President of Enterprise Fraud Management at SunTrust Bank; Transcript of SSN Workshop (Dec. 11, 2007) at 170-71, Remarks of Joel Winston, Associate Director, Division of Privacy and Identity Protection, Federal Trade Commission.
- 52 FTC Staff Summary, at 20, 23-25.
- 53 See FTC Staff Summary, at 12. Five percent of all identity theft victims point to a stolen wallet as the source of information used to commit the identity theft against them. Notably, 56 percent of all victims do not know how their information was obtained by the thief. See FTC Identity Theft Survey, at 30.
- 54 FTC Staff Summary, at 12.

- 
- 55 See, e.g., Lena H. Sun, *Posting of Social Security Numbers Results in Suspension of Three Workers*, Washington Post, June 15, 2008, available at <http://www.washingtonpost.com/wp-dyn/content/article/2008/07/14/AR2008071402245.html> (reporting that the Social Security numbers of nearly 4,700 current and former District of Columbia Metro employees were mistakenly posted on the transit agency's website).
- 56 FTC Staff Summary, at 40; Transcript of SSN Workshop (Dec. 10, 2007) at 96, Remarks of Jim Davis, Associate Vice Chancellor for Information Technology & CIO, University of California-Los Angeles; Transcript of SSN Workshop (Dec. 10, 2007) at 88-89, Remarks of Kimberly Gray, Chief Privacy Officer for Highmark, Inc.
- 57 See Cal. Civ. Code § 1798.85.
- 58 See Government Accountability Office, GAO-08-1009R, *Social Security Numbers Are Widely Available in Bulk and Online Records, but Changes to Enhance Security Are Occurring*, 4 (Sept. 2008) (approximately 25 states have passed laws limiting the public display and/or use of SSNs); Transcript of SSN Workshop (Dec. 10, 2007) at 83-85, Remarks of Steven Sakamoto-Wendel, Assistant Attorney General, State of Maryland.
- 59 FTC Staff Summary, at 40-41; Transcript of SSN Workshop (Dec. 10, 2007) at 85-86, Remarks of Steven Sakamoto-Wendel, Assistant Attorney General, State of Maryland. Some workshop participants and commenters were concerned that certain states are beginning to move beyond public display restrictions. See Transcript of SSN Workshop (Dec. 10, 2007) at 160, Remarks of Robert F. Ryan, Vice President for Government Affairs, TransUnion; Transcript of SSN Workshop (Dec. 10, 2007) at 181-82, Remarks of Michael Lamb, Vice President and General Counsel, LexisNexis Risk and Information Analytics Group (commenting on a recent Minnesota law mandating fairly broad sale and use restrictions in addition to restrictions on display of full SSNs).
- 60 FTC Staff Summary, at 23-26; Transcript of SSN Workshop (Dec. 10, 2007) at 93-95, Remarks of Kimberly Gray, Chief Privacy Officer for Highmark, Inc. (discussing the removal of SSNs from Highmark, Inc. identification cards and the various ways Highmark, Inc. continues to use SSNs for data matching); Transcript of SSN Workshop (Dec. 10, 2007) at 103-104, Remarks of Jim Davis, Associate Vice Chancellor for Information Technology & CIO, University of California-Los Angeles (explaining that although the university has removed SSNs from its identification cards and dramatically reduced their use, there are some instances where SSNs remain necessary for data matching).
- 61 See, e.g., Comment of Mortgage Bankers Assoc., at 4 (recommending the use of truncated SSNs as a way to limit identity theft exposure); Comment of New York State Consumer Protection Board, at 2 (recommending the use of truncated SSNs on all documents as a way of preventing identity theft); Transcript of SSN Workshop (Dec. 10, 2007) at 107, Remarks of Kim Duncan, Vice President of Enterprise Fraud Management, SunTrust Bank (discussing the use of SSN truncation by financial institutions).
- 62 See Government Accountability Office, GAO-06-495, *Social Security Numbers: Internet Resellers Provide Few Full SSNs, but Congress Should Consider Enacting Standards for Truncating SSNs*, 12-14 (May 2006).
- 63 See, e.g., Comment of Consumers Union, at 3.
- 64 Many of the current congressional proposals addressing SSNs include display restrictions. See, e.g., Social Security Number Misuse Prevention Act, S. 238, 110th Cong. § 3 (2007); Social Security Number Privacy and Identity Theft Protection Act of 2007, H.R. 3046, 110th Cong. §§ 2 & 8 (2007).

- 65 See Cal. Civ. Code § 1798.85.
- 66 See 16 C.F.R. Part 314; 17 C.F.R. § 248.30; Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8,616 (Feb. 1, 2001).
- 67 See *Identity Theft: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. (June 16, 2005) (written statement of Federal Trade Commission) at 7. The Task Force similarly recommended such standards. See Strategic Plan, at 35.
- 68 FTC Staff Summary, at 42; Transcript of SSN Workshop (Dec. 10, 2007) at 186, Remarks of Dr. Annie I. Anton, Associate Professor, North Carolina State University, and Director, PrivacyPlace.org; Transcript of SSN Workshop (Dec. 11, 2007) at 51, Remarks of Stuart Pratt, President and CEO, Consumer Data Industry Association.
- 69 See *Identity Theft: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. (June 16, 2005) (written statement of Federal Trade Commission) at 7. The Task Force also supported this recommendation, as well as civil penalty authority to enforce such standards. See Strategic Plan, at 34-35, 37.
- 70 Strategic Plan, at 34-35; FTC Staff Summary, at 41-42.
- 71 The federal banking agencies and the NCUA have issued guidance to their regulated entities regarding breach response and notification procedures. See Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736 (Mar. 29, 2005).
- 72 Transcript of SSN Workshop (Dec. 11, 2007) at 106, Remarks of James Lewis, Senior Fellow and Director of the Technology and Public Policy Program, Center for Strategic and International Studies; Transcript of SSN Workshop (Dec. 10, 2007) at 226, Remarks of Emily Mossburg, Senior Manager, Security and Privacy Services, Deloitte & Touche; Transcript of SSN Workshop (Dec. 10, 2008) at 96-97, Remarks of Jim Davis, Associate Vice Chancellor for Information Technology & CIO, University of California-Los Angeles; Transcript of SSN Workshop (Dec. 11, 2007) at 51, Remarks of Stuart Pratt, President and CEO, Consumer Data Industry Association.
- 73 Transcript of SSN Workshop (Dec. 11, 2007) at 106, Remarks of James Lewis, Senior Fellow and Director of the Technology and Public Policy Program, Center for Strategic and International Studies; Transcript of SSN Workshop (Dec. 10, 2007) at 143, Remarks of Jim Davis, Associate Vice Chancellor for Information Technology & CIO, University of California-Los Angeles; Transcript of SSN Workshop (Dec. 10, 2007) at 46-47 and (Dec. 11, 2007) at 110-12, Remarks of Chris Hoofnagle, Senior Staff Attorney, Samuelson Law, Technology and Public Policy Clinic, UC Berkeley School of Law.
- 74 FTC Staff Summary, at 41; Strategic Plan, at 34-35.
- 75 See, e.g., "Deter, Detect, Defend: Avoid ID Theft," Federal Trade Commission, available at <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth01.pdf>.
- 76 See, e.g., FTC Staff Summary, at 23-26; Transcript of SSN Workshop (Dec. 10, 2007) at 111-13, 117-18, Remarks of Bill Schaumann, Senior Manager, Ernst & Young.



Appendix 3

*Information Security Policy* (City of Chicago, February 15, 2008)

City of Chicago

## Information Security Policy



**Hardik Bhatt**  
**Chief Information Officer**

## Table of Contents

I.	Introduction .....	3
II.	Purpose .....	3
III.	Scope .....	3
IV.	Definitions .....	3
V.	Organizing Information Security .....	4
VI.	Asset Management .....	4
VII.	Human Resources Security .....	7
VIII.	Communications and Operations Management .....	8
IX.	Access Control .....	9
X.	Information Security Incident Management .....	11
XI.	Compliance .....	12
	Appendix A – Common Terms and Definitions .....	13
	Appendix B – Change Control .....	14

## **I. Introduction**

- A. The City of Chicago (City) intends to manage its information technology and information assets to maximize their efficient, effective, and secure use in support of the City's business and its constituents.
- B. This document, the Information Security Policy (Policy), defines the governing principles for the secure operation and management of the information technology used, administered, and/or maintained by the City and for the protection of the City's information assets.
- C. Violations of the City's Information Security Policy must be reported to Department Management or the Department of Innovation and Technology's (DoIT) Chief Information Officer.

## **II. Purpose**

- A. To define the responsibilities of the City's officers, employees, agents, departments, commissions, boards, offices, and agencies with respect to appropriate use and protection of the City's information assets and technology.
- B. To ensure that the City's information assets and technology are secure from unauthorized access, misuse, degradation, or destruction.

## **III. Scope**

- A. This Information Security Policy applies to the City of Chicago, its departments, commissions, boards, offices, and agencies, and all officers, employees, temporary employees, interns, vendors, consultants, contractors and agents thereof--collectively referred to as "User(s)". The principles set forth in this Policy are applicable to all information technology and assets, in all formats, used by the City.
- B. This Policy does not create any rights, constitute a contract, or contain the terms of any employment contract or other contract between the City of Chicago, any employee or applicant for employment, or any other person. Rather, this Policy details certain purposes, procedures, guidelines, responsibilities, and other matters the City of Chicago deems relevant to its management of information assets. The City reserves the right to amend this Policy or any part or provision of it.

## **IV. Definitions**

Please familiarize yourself with the definitions in appendix A as part of your understanding of this Information Security Policy.

## **V. Organizing Information Security**

### **A. Information Security Co-ordination**

The Department of Innovation and Technology is responsible for designing, implementing and maintaining a City-wide information security program--in conjunction with other departments--and for assisting all City departments, agencies, offices, boards, and commissions in implementing and maintaining information management practices at their respective locations.

### **B. Allocation of information security responsibilities**

The City's Chief Information Officer (CIO) is responsible for overall security of information assets and technology at the City. The CIO may delegate specific responsibilities related to information security to others within the City based on their job function.

### **C. Confidentiality Agreements**

Employees, consultants, or contractors who use the City's information technology are required to read, understand, and agree to the City's Confidentiality and Acceptable Use Agreement regarding their responsibilities and conduct related to the protection of the City's information assets and technology.

### **D. Third Parties**

The City often utilizes third parties in support of delivering business services. When, as a result, these arrangements extend the City's information technology enterprise or business processes into the third parties' computing environments—for example, in cases of Application Service Providers (ASPs)—the third parties must abide by this Policy, as applicable, unless specific additional provisions have been established through contractual agreements.

## **VI. Asset Management**

### **A. Information Classification**

The City's information, whether in electronic or physical form, can be categorized into three classifications. Due care must be taken to protect the City's information assets in accordance with the three classifications, as described within this Policy.

1. Confidential – Sensitive personally identifiable information (PII) used for business purposes within the City which, if disclosed through unauthorized means, could adversely affect the City's personnel, including employees and constituents, and could have legal, statutory, or regulatory repercussions. Examples include: information exempt from

## Information Security Policy

disclosure under the Illinois Freedom of Information Act (FOIA), information protected from disclosure under the federal Health Insurance Portability and Accountability Act (HIPAA), other personnel information including Social Security numbers, and personal financial information including credit card data protected by the Payment Card Industry's Digital Security Standard (PCI DSS).

2. Internal – Information related to the City's business that if disclosed, accessed, modified or destroyed by unauthorized means, could have limited or significant financial or operational impact on the City. Examples include: strategic plans, vendors' proprietary information, responses to Requests for Proposals (RFPs), information protected by intergovernmental non-disclosure agreements or other non-disclosure agreements, and design documents. Other information related to the City's information technology that is considered Internal includes dial-up modem phone numbers and access point Internet Protocol (IP) addresses.
3. Public – Information intended for unrestricted public disclosure in the course of the City's business. Examples include: press releases, public marketing materials, and employment advertisements.

### B. Responsibility for Assets

#### 1. Ownership of Assets

All information stored and processed over the City's technology systems is the property of the City. Users of the system have no expectation of privacy associated with the information they store in or send through these systems, within the limits of the federal, state and local laws of the United States and, where applicable, foreign laws.

#### 2. Acceptable and Unacceptable Use of Assets

- a. To effectively conduct the City's business and operations, the City makes available to authorized employees and third parties various information technology resources, including e-mail, the City's Intranet, the Internet, and other communication and productivity tools. Use of these resources is intended for business purposes in accordance with Users' job functions and responsibilities, with limited personal use permitted only in accordance with the City's Ethics Ordinance, personnel rules, this policy, and other applicable City policies. The limited personal use of information technology resources is not permissible if it creates a non-negligible expense to the City, consumes excessive time, or violates departmental policy. The privilege of limited personal use may be revoked or limited at any time by the City or department officials.
- b. Users must not allow any consultant, visitor, friend, family member, customer, vendor or other unauthorized person to use their network account, e-mail address or other

## Information Security Policy

City-provided computer facilities. Users are responsible for the activities performed by and associated with the accounts assigned to them by the City.

- c. No User may use City-provided Internet or Intranet access or the City's Confidential or Internal information to solicit or conduct any personal commercial activity or for personal gain or profit or non-City approved solicitation.
- d. Users must not make statements on behalf of the City or disclose Confidential or Internal City information unless expressly authorized in writing by their Department Management. This includes Internet postings, or bulletin boards, news groups, chat rooms, or instant messaging.
- e. Users must protect Confidential or Internal information being transmitted across the Internet or public networks in a manner that ensures its confidentiality and integrity between a sender and a recipient. Confidential information such as Social Security numbers, credit card numbers, and electronic Protected Health Information (ePHI) must be transmitted using encryption software.
- f. Internal information such as email lists must not be posted to any external information source, listed in telephone directories, placed on business cards, or otherwise made available to third parties without the prior express written permission of the User's Department Management.
- g. Users must not install software on the City's network and computer resources without prior express written permission from the Department of Innovation and Technology. Person-to-person (P2P) applications, Voice over IP (VOIP), instant messenger (IM) applications, and remote access applications pose an especially high risk to the City and their unauthorized use is strictly prohibited. City business must not be conducted on any device that allows P2P communication (such as file sharing music applications) without explicit approval from the Department of Innovation and Technology.
- h. Users must not copy, alter, modify, disassemble, or reverse engineer the City's authorized software or other intellectual property in violation of licenses provided to or by the City. Additionally, Users must not download, upload, or share files in violation of U.S. patent, trademark, or copyright laws. Intellectual property that is created for the City by its employees, vendors, consultants and others is property of the City unless otherwise agreed upon by means of third party agreements or contracts.

## Information Security Policy

- i. Users must not access the Internet, the Intranet or e-mail to use, upload, post, mail, display, or otherwise transmit in any manner any content, communication, or information that, among other inappropriate uses:
  - i. interferes with official City business;
  - ii. is hateful, harassing, threatening, libelous or defamatory, pornographic, profane, or sexually explicit;
  - iii. is deemed by the City to offend persons based on race, ethnic heritage, national origin, sex, sexual orientation, age, physical or mental illness or disability, marital status, employment status, housing status, religion, or other characteristics that may be protected by applicable civil rights laws;
  - iv. impersonates a person (living or dead), organization, business, or other entity;
  - v. enables or constitutes gaming, wagering or gambling of any kind;
  - vi. promotes or participates in unauthorized fundraisers;
  - vii. promotes or participates in partisan political activities;
  - viii. promotes or participates in unauthorized advertising of City projects and any advertising of private projects;
  - ix. compromises or degrades the performance, security, or integrity of the City's technology resources and information assets;
  - x. contains a virus, logic bomb, or malicious code;
  - xi. constitutes participation in chain letters, unauthorized chat rooms, unauthorized instant messaging, spamming, or any unauthorized auto-response program or service.

## VII. Human Resources Security

### A. Prior to Employment

All employees, consultants, and contractors who use of the City's information technology as part of their job function are required to sign the City's Confidentiality and Acceptable Use Agreement.

### B. During Employment

#### 1. Information Security Awareness, Education, and Training

Security Awareness begins during the hiring process and it is the responsibility of the User to remain aware of current security policies. The City's Intranet site contains the City's Security Policies as well as educational materials such as the "Security First" presentation. Users should read the Security Reminders that are periodically distributed



## Information Security Policy

by email. Users must also respond to the Information Security Notice that is displayed while logging on to City related systems.

### 2. Disciplinary Process

Any violation of this Policy, or any Part or provision hereof, may result in disciplinary action, including termination and/or civil action and/or criminal prosecution.

### C. Termination or Change of Employment

#### 1. Return of Assets

When a User leaves the City, all Information Assets remain the property of the City. A User must not take away such information or take away a copy of such information when he or she leaves the City without the prior express written permission of the City.

#### 2. Removal of Access Rights

Upon termination of an employee or vendor, the person who requested access to technology resources must request the termination of that access using the City's access request procedure. In the event that the requestor is not available, the responsibility is placed upon the manager of the employee or vendor. The City may automatically disable or delete accounts where termination is suspected even if formal notification was by-passed.

## VIII. Communications and Operations Management

### A. Protection Against Malicious Code

1. It is the City's policy to conduct virus scanning of its technology resources to protect them from the threat of malicious code. The City will intercept and/or quarantine any networking and computer resource that poses a virus threat to its information assets.
2. All servers and workstations (networked and standalone) must have the City's approved antivirus protection software installed, properly configured, and functioning at all times. Additionally, systems that have not been issued by the City but that use the City's network must also be protected by antivirus software.
3. All incoming and outgoing e-mails must be scanned for viruses.
4. Users are responsible for ensuring that software, files, and data downloaded onto the City's workstations are properly scanned for viruses.
5. Users must conduct virus scans on all external media received or used by the City.
6. Users must ensure that all workstations (networked and standalone) have the most current antivirus signature files loaded.

## Information Security Policy

### B. Back-Up

1. The City will perform regular backups of User files stored on the City's file servers and storage media that are centrally managed by the Department of Innovation and Technology. This process will be coordinated in conjunction with the City's User departments based on their individual business needs.
2. The City will not back up multimedia files in formats including, but not limited to, .mp3, m4a, m4p .avi and .mov.

### C. Media Handling

#### 1. Disposal of Media

Except as otherwise provided by law or court order, electronic information maintained in a department's office will be destroyed by department staff or the Department of Innovation and Technology when the retention period expires, in compliance with the City's implementation of the State of Illinois Local Records Act.

### D. Monitoring

#### 1. Monitoring System Use

- a. Users should have no expectation of privacy in their use of Internet services provided by the City. The City reserves the right to monitor for unauthorized activity the information sent, received, processed or stored on City-provided network and computer resources, without the consent of the creator(s) or recipient(s). This includes use of the Internet as well as the City's e-mail and instant messaging systems.
- b. All information technology administrators, technicians and any other employees who by the nature of their assignments have privileged access to networks or computer systems must obtain written approval from the Department of Innovation and Technology to monitor User activity.

#### 2. Clock Synchronization

All server clocks must be synchronized in a manner approved by the Department of Innovation and Technology in order to provide for timely administration and accurate auditing of systems.

## IX. Access Control

### A. User Access Management

#### 1. User Account Management

- a. Access to Confidential and Internal data must be made using a formal Access Request Form.

## Information Security Policy

- b. User accounts that have not been used for 90 days may be disabled without warning. After 180 days of inactivity, these accounts may be deleted without warning.
- c. Departments must use the access request process to notify the Department of Innovation and Technology of a change in employment status (such as when a User takes a leave of absence, transfers departments, or is terminated). The account of a User on a leave of absence can be retained, suspended, or deleted at the discretion of the User's department.

### B. User Responsibilities

#### 1. Password Use

- a. All e-mail, network, domain accounts must be password protected. All new accounts will be created with a temporary password. The temporary password must be changed upon first use.
- b. Mobile devices must be password protected; this includes but is not limited to personal digital assistants (PDA), smart phones, laptops, handhelds (e.g. Blackberries) and off-site desktops.
- c. Passwords used on the City's systems and on non-City systems that are authorized for use must have the following characteristics unless otherwise approved by the Department of Innovation and Technology:
  - i. Passwords must be a minimum of 8 characters in length;
  - ii. Passwords must contain both alphabetic and numeric characters;
  - iii. Passwords must not be the same as the username;
  - iv. Passwords must not contain proper names or words taken from a dictionary;
  - v. Passwords must be changed at minimum every 90 days; and,
  - vi. Passwords used for production systems must not be the same as those used for corresponding non-production system such as the password used during training.
- d. Passwords must not be disclosed to anyone. All passwords are to be treated as Confidential information.

#### 2. Screen Savers

Use of password-protected screen savers is recommended to prohibit unauthorized system access. Screen savers should initiate after 10 minutes of inactivity. Password-protected screen savers are required on workstations that access Confidential information such as electronic Protected Health Information. Password-protected screen savers are also required on workstations that access Internal information if the workstation is not in an area that has restricted access.

C. Mobile Computing and Remote Access

1. Laptops, off-site computers, and mobile media that contain Confidential information must be encrypted using an encryption technique approved by the Department of Innovation and Technology. Mobile media that contain Internal information must be protected using an encryption technique approved by the Department of Innovation and Technology, a strong logon password, or restricted physical access in order to protect the data. Examples of mobile media include flash drives, DVDs, CDs, and external hard drives.
2. Personal media devices (for example, MP3 players such as iPods) must not be used as peripheral devices on City-issued workstations.
3. Remote access is provided by the City as an information conduit to assist in the accomplishment of municipal duties and goals. Any other use is strictly prohibited. Requests for remote access must have a valid business reason and be approved by the Department of Innovation and Technology.
4. All remote access connections must be through a secure, centrally administered point of entry approved by the City. Authorized remote access connections must be properly configured and secured according to City-approved standards including the City's password policy. All remote desktop protocol implementations must be authorized by the Department of Innovation and Technology. Remote access through unapproved entry points will be terminated when discovered.
5. Non-City owned computer equipment used for remote access must be approved and must also comply with the City's standards. The City will not be responsible for maintenance, repair, upgrades or other support of non-City owned computer equipment used to access the City's network and computer resources through remote access services.
6. Users who utilize workstations that are shared with individuals who have not signed a Confidentiality Agreement with the City must ensure that the City's data is removed or deleted after each use.

## **X. Information Security Incident Management**

A. Reporting Information Security Events and Weaknesses

1. Violations of the City's Information Security Policy or any or all parts or provisions of this Policy must be reported to Department Management or to the Department of Innovation and Technology.
2. Users must ensure that a Help Desk representative is notified immediately whenever a security incident occurs. Examples of security incidents include a virus outbreak,

## Information Security Policy

defacement of a website, interception of email, blocking of firewall ports, and theft of physical files or documents.

3. All reports of alleged violations of this Policy, or any part or provision hereof, will be investigated by the appropriate authority. During the course of an investigation, access privileges may be suspended.

## **XI. Compliance**

### **A. Compliance with Legal Requirements**

#### **1. Intellectual Property Rights**

- a. Intellectual Property that is created for the City by its employees is property of the City unless otherwise agreed upon by means of third party agreements or contracts.
- b. No User may transmit to, or disseminate from, the Internet any material that is protected by copyright, patent, trademark, service mark, or trade secret, unless such disclosure is properly authorized and bears the appropriate notations.

#### **2. Prevention of Misuse of Information Processing Facilities**

Users are prohibited from using the City's processing facilities—including data centers, network cabinets or closets, and other facilities housing the City's technology equipment—in any way that violates this Policy, and federal, state, or municipal law, including, but not limited to, the City's Municipal Code and Personnel Rules.

#### **3. Compliance with Relevant Laws and Regulations**

By virtue of the City's services to its constituents and the nature of its legal status, the City is covered by certain laws and regulations dealing with security and privacy of information, most notably the Illinois Personal Information Protection Act (PIPA), the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry's Digital Security Standard (PCI DSS). These laws and regulations, in some circumstances, may require additional safeguards for protection the City's information beyond the stipulations of this Policy. (For example, when accessing credit/debit cardholder data remotely, it is never to be stored on local hard drives, floppy disks, or external media. Furthermore, cut-and-paste and print functions are prohibited during remote access sessions.) Accordingly, Users with access to Protected Health Information (PHI) must abide by HIPAA and Users with access to credit/debit card information must abide by PCI, as applicable.

#### **4. Compliance with Security Policies and Standards**

All Users must read and sign the City's Compliance and Acceptable Use Agreement prior to being authorized to access the City's information technology and information assets.

## Appendix A – Common Terms and Definitions

1. **Computer Resources** - All related peripherals, components, disk space, system memory and other items necessary to run computer systems.
2. **Credit Card Data** - The Primary Account Number (PAN), Card Verification Value (CVV--the 3-4 digit code on the signature block on the back of a Credit Card), track data (the data read directly from the magnetic stripe of a Credit Card) and PIN Block data (also read from the magnetic stripe). The PCI DSS can be found at <https://www.pcisecuritystandards.org>.
3. **Department Management** - A supervisor, manager, director, commissioner, or other officer or employee of the City designated by a City agency, board, commission, department, or office to be responsible for implementation of this Policy by his/her City agency, board, commission, department, or office.
4. **Electronic Mail (E-mail)** - The transmission of messages through electronic means in a body or attachment using the City's network or other information technology.
5. **Information Assets** - Information and data created, developed, processed, or stored by the City that has value to the City's business or operations.
6. **Information Technology or Network and Computer Resources** - Computer hardware and software, network hardware and software, e-mail, voice mail, video conferencing, facsimile transmission, telephone, remote access services, printers, copiers, and all other printed and electronic media.
7. **Intranet** - The suite of browser-based applications and HTML pages that are available for use only with access to the City's internal network.
8. **Internet** - The worldwide 'network of networks' connected to each other using the IP protocol and other similar protocols. The Internet enables a variety of information management services, including, but not limited to, e-mail, instant messaging, file transfers, file uploads, file downloads, news, and other services.
9. **Internet Services** - Any service in which its primary means of communication is the Internet. For example e-mail, web browsing and file transfers.
10. **Mobile Computing Devices** - Mobile devices and Mobile media. Mobile data processing devices are used as business productivity tools. Examples include: laptops, personal digital assistants (PDAs), smart phones, handhelds (e.g. Blackberries), and off-site desktops. Mobile media are devices typically used to transport data. Examples include: flash drives, DVDs, CDs, and external hard drives.
11. **Network** - The linking of multiple computers or computer systems over wired or wireless connections.
12. **P2P** - Peer-to-Peer network. A network where nodes simultaneously function as both "clients" and "servers" to other nodes on the network, P2P may be used for a variety of uses, but it is typically used to share files such as audio files. Examples of P2P networks include Napster, KaZaA, and LimeWire. If a node is not properly configured, any file on the device may potentially be accessed by anyone on the network.
13. **Protected Health Information** - Individually identifiable health information about an individual that relates to the past, present, or future physical or mental health or condition, provision of health care, or payment for health care.
14. **Remote Access Services** - A service that enables off-site access to the City information technology and assets. Examples include the City's telephone exchanges, internal phone switches, wireless access points (WAP), and Virtual Private Network (VPN) connections. Remote access includes, but is not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems.
15. **Security Incident** - An event that has an adverse impact on the confidentiality, integrity, and availability of computer systems, computer networks, electronic information assets, or physical information assets.
16. **User(s)** - The City's departments, commissions, boards, offices, officers, employees, temporary employees, interns, vendors, consultants, contractors, and authorized agents who utilize the City's information assets and technology.
17. **World Wide Web (WWW)** - Browser-based applications and HTML pages that are available for access and use across the Internet.

## Appendix B – Change Control

Version Number	Date of Change	Authors	Description Change
1.0	9/2004	Unknown	Original Document
2.0	01/2006	Unknown	Changed version and day on page 7, added the sentence that begins with "Passwords must not be shared..." on page 14, removed potential implication that passwords may be shared with authorization on page 14.
3.0	10/2007	BIS	The Information Management Policy V 2 was modified and renamed to Information Security Policy V 3. Information Management Policy and Information Security Policy are used as synonyms within the City of Chicago. In Version 3, there have been numerous document updates including re-arrangement of content and removal of duplicate or outdated language. Version 3 is the official policy used by BIS as of 10/2007.
3.1	01/2008	DoIT	Changed BIS references to DoIT.
3.2	01/2008	DoIT	Minor corrections (spelling etc).
3.3	01/2008	DoIT	Edited VI B 2 a and i for Internet Acceptable Use and small format changes including TOC.
3.4	01/2008	DoIT	Removed newsgroup and mail list blanket constraint.
3.5	01/2008	DoIT	General cleanup and removed reference to raffles.
4	02/2008	DoIT	Citywide Review Completed. Only small format change was made.

Appendix 4

*Attorney General Security Breach Notification Guidance* (Vermont  
Attorney General's Office, April 24, 2007)



## Attorney General Security Breach Notification Guidance

This Guidance describes the steps that a business or state agency shall take in the event that the business or state agency suspects that its computerized data or systems containing “personal information”, as set forth in the statute, has been subject to a security breach.

The Security Breach Notice Act, codified at 9 V.S.A. Sections 2430 and 2435, became effective on January 1, 2007. This law requires businesses and state agencies to notify consumers in the event that the business or state agency suffers a “security breach”, defined as the **unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the state agency or business.** 9 V.S.A. Section 2430(8). The law provides that businesses and state agencies do not need to give notice where they determine that misuse of personal information is not reasonably possible, and they so inform the Vermont Attorney General’s Office.

“Personal information” that is subject to the law is defined as:

an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons:

- (i) Social Security number;
- (ii) Motor vehicle operator’s license number or nondriver identification card number;
- (iii) Financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords;
- (iv) Account passwords or personal identification numbers or other access codes for a financial account.

9 V.S.A. Section 2430(5). The statute further requires that notice be sent to affected consumers following discovery of or notification about the breach “in the most expedient time possible and without unreasonable delay”, consistent with the needs of law enforcement. 9 V.S.A. Section 2435(b).

You, as a business or state agency, shall take the following steps if you suffer from a security breach. Review all steps immediately, and take as many of the detailed steps as possible, as quickly as possible.

### 1. Secure the data immediately.

- a. Call your head of computer operations or information technology to find out what steps must be taken to secure the data. Take all appropriate measures to secure the data, including possibly taking the computer server off line or isolating the data.

- b. Do NOT attempt to determine whether the data has been compromised until law enforcement has approved the steps you plan to take.
- c. See Appendix 1 for a description of some of the steps that should be taken in the event of a security breach to secure the data.

**2. Involve Law Enforcement immediately.**

- a. Call the state police or FBI to report the incident and determine next steps. If you are a Vermont-based business or state agency, or the data at issue is housed in Vermont, call:

FBI: During normal business hours, call the Burlington FBI office at: 802-863-6316.  
After normal business hours, call the Albany FBI office at 518-465-7551.

State Police: Bureau of Criminal Investigation 802-241-5350

If your business or agency is located out of state and the data at issue is housed out of state, call the FBI, state police or other appropriate law enforcement agency in your area.

- b. Inform the FBI or state police of your obligation to notify consumers of the breach **within 10 business days**. If either the FBI or state police requests a delay in notification for purposes of a law enforcement investigation, the request must be made in writing or you must document the request contemporaneously, noting the name of the law enforcement officer making the request and the name of the officer's agency.
- c. If either the FBI or state police requests a delay in notification for purposes of a law enforcement investigation, prepare your notification to consumers so that you can send it immediately upon hearing that the delay is no longer needed. (See Step 5 below.)
- d. The law enforcement agency making a request for delay is responsible for promptly notifying you when the law enforcement agency believes that delay will no longer impede the law enforcement investigation. Until you are notified that the delay is no longer needed, you must contact the responsible law enforcement officer every 15 days to determine that the delay is still required.
- e. After the law enforcement agency notifies you that the delay is no longer needed, **immediately** send your notice to consumers.
- f. It should not be necessary for law enforcement to complete its investigation before notice to affected consumers can be sent.

**3. Contact any entities from which you may have obtained the data immediately.**

- a. If you received the data from other entities, such as banks or other states, contact these entities as they may have their own obligations to notify consumers about the security breach.

**4. Notify the Vermont Attorney General's Office about the breach.**

- a. Call the Vermont Attorney General's Office to inform the Attorney General about the breach by contacting:

Julie Brill, Vermont Assistant Attorney General  
Chris Rouleau, Vermont Attorney General Investigator  
802-828-5479

**5. Notify consumers about the breach WITHIN 10 BUSINESS DAYS OF DISCOVERY.**

- a. If law enforcement does not request a delay in notification to consumers, you must notify consumers about the breach **within 10 business days of discovery of the breach**.
- b. The notice should contain the following information :
- A general description of the unauthorized access or acquisition.
  - The type of personal information affected.
  - A general description of the steps you will take to protect the information from further unauthorized access or acquisition.
  - Your toll-free telephone number that consumers may call for further information and assistance.
  - Advice that directs the consumer to remain vigilant by reviewing account statements and obtaining free credit reports from each credit reporting agency to determine if there is suspicious activity such as new accounts being opened in the consumer's name. Consumers in Vermont are entitled to two free credit reports each year from each credit reporting agency. The Attorney General's website has information about free credit reports available to Vermonters:  
[http://www.atg.state.vt.us/upload/1120132977\\_How\\_to\\_Get\\_Free\\_Credit\\_Reports.pdf](http://www.atg.state.vt.us/upload/1120132977_How_to_Get_Free_Credit_Reports.pdf)
- c. A model letter is provided for you to use. See Appendix 2. The model letter is designed to be used when you do not know whether the consumer's information has been misused. If you are aware that the consumer's information has been misused, then a more specific letter must be sent, outlining how the information has been misused and

recommending that the consumer take immediate action to guard against identity theft.

- d. Consider whether you will offer credit monitoring services to the consumers. These are services offered by credit reporting agencies to determine if there is suspicious activity such as new accounts being opened in the consumer's name. While not required by law, many companies and agencies that experience breaches provide credit monitoring services to consumers.
- e. Send the notice in one of the following ways.
  - 1. Direct notice to consumers through:
    - i. A mailing to the consumer's residence; or
    - ii. The telephone, provided the telephone contact is directly made with each consumer, and not through a pre-recorded message; or
    - iii. Electronic notice via email (Note: it is difficult to qualify to use electronic notice. See 9 V.S.A. Section 2435(b)(5)(A)ii.);
  - 2. Substitute notice is allowed if you can demonstrate one of the following:
    - (1) providing direct notice through the mail or telephone would cost more than \$5,000;
    - (2) the group of consumers affected by the security breach exceeds 5,000; or
    - (3) the data collector does not have sufficient contact information to provide notice via the mail or telephone.

If you satisfy one of the three criteria for substitute notice, then you may provide notice to affected consumers by doing **both** of the following:

- i. prominently placing the notice on your website if you have one; **and**
  - ii. sending a press release with all the information to be contained in the notice to major statewide and regional media.
- f. Whichever mechanism of distribution you use, the notice must contain all the elements outlined in 4.b above.

6. **Notify the three major credit reporting agencies if you are going to send a notice of security breach to more than 1,000 consumers. This notice to credit reporting agencies shall be sent no later than the same day as the notices are sent to consumers.**

- a. The notification to the credit reporting agencies should be sent to the following addresses:

- **Equifax**

U.S. Consumer Services  
Equifax Information Services, LLC  
Phone: 678-795-7971  
Email: [businessrecordsecurity@equifax.com](mailto:businessrecordsecurity@equifax.com)

- **Experian**

Experian Security Assistance  
P.O. Box 72  
Allen, TX 75013  
Email: [BusinessRecordsVictimAssistance@experian.com](mailto:BusinessRecordsVictimAssistance@experian.com)

- **TransUnion**

Phone: 1-800-372-8391  
Email: [fvad@transunion.com](mailto:fvad@transunion.com)

7. **Notice of a security breach is not required if you determine that misuse of personal information is not reasonably possible, and you so inform the Vermont Attorney General's Office within 10 business days of the security breach.**

- a. If you establish that misuse of the data is not reasonably possible, then you may forgo notifying affected consumers about the breach *as long as* you provide a detailed explanation of your determination to the Attorney General's Office within 10 business days of the breach. The explanation should be provided to the following: Consumer Protection Unit, Vermont Attorney General's Office, 109 State Street, Montpelier, Vermont 10609-1001.
- b. You may designate your explanation as "trade secret" if it meets the definition of trade secret under 1 V.S.A. Section.317(c)(9).
- c. If you learn, after notifying the Attorney General's Office, that misuse of the personal information has occurred or is occurring, then you shall provide, pursuant to the provisions of this Guidance, notice of the security breach to affected consumers **within 10 business days of receiving such information.**

**8. This Guidance does not apply to certain financial institutions and certain other businesses subject to regulation by the Department of Banking, Insurance, Securities and Health Care Administration (BISHCA).**

The Guidance does not apply to: (1) a person or entity licensed or registered with BISHCA under Titles 8 or 9 of the Vermont Statutes Annotated, however, such person or entity is subject to guidance, bulletins, and regulations issued by BISHCA; or (2) a financial institution, bank, or credit union that is subject to either: (A) The Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, as such federal guidance may be revised from time to time; or (B) The Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14, 2005, by the National Credit Union Administration, as such federal guidance may be revised from time to time.

## **APPENDIX 1**

### **Procedures the Computer User Should Institute Both Prior to Becoming a Computer Crime Victim and After a Violation Has Occurred**

Guidance from the FBI National Computer Crime Squad  
[www.emergency.com/fbi-nccs.htm](http://www.emergency.com/fbi-nccs.htm)

- Place a login banner to ensure that unauthorized users are warned that they may be subject to monitoring
- Turn audit trails on.
- Consider keystroke level monitoring if adequate banner is displayed.
- Request trap and tracing from your local telephone company.
- Consider installing caller identification.
- Make backups of damaged or altered files.
- Maintain old backups to show the status of the original.
- Designate one person to secure potential evidence.
- Evidence can consist of tape backups and printouts. These should be initialed by the person obtaining the evidence. Evidence should be retained in a locked cabinet with access limited to one person.
- Keep a record of resources used to reestablish the system and locate the perpetrator.

### **Reporting a Computer Crime to Law Enforcement**

Guidance from the California Highway Patrol Computer Crimes  
Investigation Unit  
[www.chp.ca.gov/html/computercrime.html](http://www.chp.ca.gov/html/computercrime.html)

When reporting a computer crime be prepared to provide the following information:

- Name and address of the reporting agency.
- Name, address, e-mail address, and phone number(s) of the reporting person.
- Name, address, e-mail address, and phone number(s) of the Information Security Officer (ISO).
- Name, address, e-mail address, and phone number(s) of the alternate contact (e.g., alternate ISO, system administrator, etc.).
- Description of the incident.
- Date and time the incident occurred.
- Date and time the incident was discovered.

- Make/model of the affected computer(s).
- IP address of the affected computer(s).
- Assigned name of the affected computer(s).
- Operating System of the affected computer(s).
- Location of the affected computer(s).

### **Incident Response DOs and DON'Ts**

#### **DOs**

1. Immediately isolate the affected system to prevent further intrusion, release of data, damage, etc.
2. Use the telephone to communicate. Attackers may be capable of monitoring E-mail traffic.
3. Immediately notify an appropriate law enforcement agency.
4. Activate all auditing software, if not already activated.
5. Preserve all pertinent system logs, e.g., firewall, router, and intrusion detection system.
6. Make backup copies of damaged or altered files, and keep these backups in a secure location.
7. Identify where the affected system resides within the network topology.
8. Identify all systems and agencies that connect to the affected system.
9. Identify the programs and processes that operate on the affected system(s), the impact of the disruption, and the maximum allowable outage time.
10. In the event the affected system is collected as evidence, make arrangements to provide for the continuity of services, i.e., prepare redundant system and obtain data back-ups. To assist with your operational recovery of the affected system(s), pre-identify the associated IP address, MAC address, Switch Port location, ports and services required, physical location of system(s), the OS, OS version, patch history, safe shut down process, and system administrator or backup.

#### **DON'Ts**

1. Delete, move, or alter files on the affected systems.
2. Contact the suspected perpetrator.
3. Conduct a forensic analysis.



## APPENDIX 2

### SAMPLE LETTER

#### To Be Used When The Breached Entity Does Not Know Whether the Consumer's Information Has Been Misused

Dear :

We are writing to you because of a recent security incident at *[name of organization]*. *[Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.]*

Below is a check list of suggestions of how you can best protect yourself in this situation.

1. **Review your bank, credit card and debit card account statements** over the next twelve to twenty-four months and immediately report any suspicious activity to your bank or credit union.
2. **Monitor your credit reports** with the major credit reporting agencies.

Equifax	Experian	TransUnion
1-800-685-1111	1-888-397-3742	1-800-916-8800
P.O. Box 740241	P.O. Box 2104	P.O. Box 1000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19022
<a href="http://www.equifax.com">www.equifax.com</a>	<a href="http://www.experian.com">www.experian.com</a>	<a href="http://www.transunion.com">www.transunion.com</a>

Under Vermont law, you are entitled to a free copy of your credit report from those agencies every twelve months. *[If you are offering consumers credit monitoring services, insert description of the services and instructions on how to access them.]*

Call the credit reporting agency at the telephone number on the report if you find:

- Accounts you did not open.
- Inquiries from creditors that you did not initiate.
- Inaccurate personal information, such as home address and Social Security number.

3. If you do find suspicious activity on your credit reports or other account statements, call your local police or sheriff's office and **file a report of identity theft**. *[Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.]* Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records, and also to access some services that are free to identity theft victims.
4. If you find suspicious activity on your credit reports or on your other account statements, consider placing a **fraud alert** on your credit files so creditors will contact you before opening new accounts. Call any one of the

three credit reporting agencies at the number below to place fraud alerts with all of the agencies.

Equifax  
800-525-6285

Experian  
888-397-3742

TransUnion  
800-680-7289

5. If you find suspicious activity on your credit reports or on your other account statements, consider placing a **security freeze** on your credit report so that the credit reporting agencies will not release information about your credit without your express authorization. A security freeze may cause delay should you wish to obtain credit and may cost some money to get or remove, but it does provide extra protection against an identity thief obtaining credit in your name without your knowledge. If you have Internet access and would like to learn more about how to place a security freeze on your credit report, please contact the Vermont Attorney General's website at: <http://www.atg.state.vt.us/display.php?smod=198>

You may also get information about security freezes by contact the credit bureaus at the following addresses:

**Equifax:**

[https://www.econsumer.equifax.com/consumer/sitepage.ehtml?forward=elearning\\_credit15](https://www.econsumer.equifax.com/consumer/sitepage.ehtml?forward=elearning_credit15)

**Experian:**

[http://www.experian.com/consumer/security\\_freeze.html](http://www.experian.com/consumer/security_freeze.html)

**TransUnion:**

<http://www.transunion.com/corporate/personal/fraudIdentityTheft/preventing/securityFreeze.page>

If you do not have Internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

6. Even if you do not find suspicious activity on your credit report or your other account statements, it is important that you **check your credit report** for the next two years. Just call one of the numbers in paragraph 2 above to order your reports or to keep a fraud alert in place.

Helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report is available on the Vermont Attorney General's website at <http://www.atg.state.vt.us>. Another helpful source is the Federal Trade Commission website, which you may find at <http://www.ftc.gov/bcp/edu/microsites/idtheft/>.

If there is anything *[name of your organization]* can do to assist you, please call *[toll-free phone number]*.

*[Closing]*

Appendix 5

*The Beacon View* (State of North Carolina Office of the State Controller  
newsletter, Summer 2007)

# THE BEACONVIEW



*"BEACON represents a new level of partnership across our State. We recognize how important BEACON will be, not just to the Department of Transportation, but for the entire State. We are excited about the opportunity to join forces for a combined system of record for personnel and payroll information."*

— Mark Foster, CFO  
Department of Transportation

## Deployment Group I Agencies

(January 2008)

Department of Administration/  
Lt. Governor's Office

Department of Correction

Department of Revenue

Department of Transportation

Governor's Office /  
Office of State  
Budget & Management

Information Technology Services

Office of State Controller

Office of State Personnel

State Board of Elections

\* All other agencies are  
scheduled to go-live  
April 2008.

STATE OF NORTH CAROLINA Office of the STATE CONTROLLER

## PROJECT BRINGS POSITIVE CHANGES FOR STATE EMPLOYEES

The demands placed on the State's human resource departments continue to grow despite limited budgets and staffing. Considering the important and often strategic roles that human resource staff members play, there is limited time for the routine tasks that fall under the management and administration of employee information.


With Employee Self Service (ESS), state employees and human resource practitioners

all win. Beginning in early 2008, state employees included in Group 1 of the BEACON HR/Payroll Project will have the opportunity to handle many of their own human resource transactions.

With minimal training and access to a computer with an internet connection, these state employees will, among other things, be able to use ESS to:

- View and print past and current pay stubs

- View available leave balances
- Enroll in the State Health Plan and for NCFlex benefits during open enrollment periods
- Securely update personal information (e.g. address, phone numbers, dependants)

Ultimately, ESS will offer a user-friendly interface that walks employees through each step of every ESS process. 

## CORE USER VOLUNTEER INSTRUCTORS BEGIN TRAINING ACTIVITIES

The BEACON HR/Payroll Project end-user training is set to kick off in early September, and the 75 people from 16 agencies across the State who have volunteered to serve as instructors are right at the center of the training efforts. These instructors, who answered a call from BEACON earlier this year, are currently taking part in extensive training themselves. Beginning in early July and continuing through the first week in

September, the instructors will spend three weeks in classroom training to prepare for the 3,000+ core users that will need training on the new system

The instructors recently completed the first phase of their training, which featured a BEACON orientation, as well as a multi-day workshop on adult learning principles. The next phase, set to begin in early August, will focus on using and understanding the SAP system. Following a half-day overview of the system and how to navigate it, instructors will receive a one-day demonstration of the processes within the system that he/she will be teaching to the core users. They will then be expected to spend 80+ hours in self-directed practice in preparation for the third and final phase of their training.

In the third phase, instructors will participate in "teach back" sessions, in which they will convey the material provided by the BEACON HR/Payroll Project Training Team to groups of other instructors. They will also take a final 2-3 day preparation course in which they will learn the final tools needed to address issues of problems, as well as any



Some of the more than 70 state employees, who volunteered to become BEACON HR/Payroll Project trainers, participate in the first phase of training in July. For a listing of all participating training volunteers, visit [www.beacon.nc.gov/...](http://www.beacon.nc.gov/)

**See Training.....Page 2**

## Training.....from Page 1

final instructions before end-user training begins for Group One agencies in September.

The BEACON HR/Payroll Project Team would like to commend these instructors for the time and effort they are investing to ensure that the system's users are prepared when the system goes live. The Team would also like to thank these individuals' managers and supervisors, as well as their agencies for their continued willingness to allow the instructors to participate in these courses and in the end-user training throughout the remainder of the project.

## PROJECT TAKES ROLE-BASED TRAINING APPROACH

**H**ave you ever spent three days in a training class only to find that you only needed the information presented in the morning of the second day? Did you feel like the rest of those days were a waste of your time? You'll be happy to know that when you come to BEACON HR/Payroll system training, your training will be focused exclusively on the information you need to know to do your job.

**T**he BEACON HR/Payroll Project Training Team is designing a role-based training approach. This

means each user will only be trained on the SAP functions that apply to his/her assigned security roles in the system. Your security roles are directly tied to the functions you will need to perform in the system in order to do your job, so you won't have to attend any training that doesn't pertain to your regular duties.

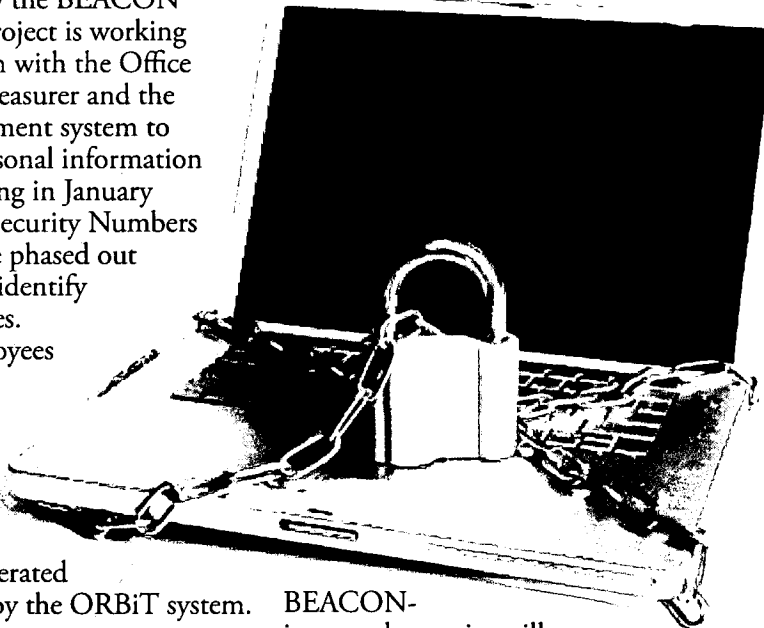
**O**nce security roles have been finalized, core human resource and payroll practitioners from throughout the State will receive training schedules, as well as information about training locations.

## PROJECT FOCUSES ON SAFEGUARDING EMPLOYEE DATA

Did you know the BEACON HR/Payroll Project is working in conjunction with the Office of the State Treasurer and the ORBiT retirement system to keep your personal information safer? Beginning in January 2008, Social Security Numbers (SSNs) will be phased out as a means to identify state employees. Instead, employees will receive an Employee ID number that is unique and is randomly generated and assigned by the ORBiT system.

This number will not only serve as your ID number during your active duty as a state employee, but it will also be your means to identify yourself in the retirement system even after you've left state government service or retired.

Employees in Group 1 and Group 2



BEACON-impacted agencies will receive their Employee ID cards in conjunction with their respective go-live dates.

For more information, visit [www.beacon.nc.gov](http://www.beacon.nc.gov) or contact BEACON at [beacon.comm@ncosc.net](mailto:beacon.comm@ncosc.net).

FOR MORE INFORMATION,  
PLEASE CONTACT:

**The BEACON HR/Payroll Change/  
Communications Team**  
919.431.6523  
[beacon.comm@ncosc.net](mailto:beacon.comm@ncosc.net)

**Robert L. Powell**  
State Controller  
919.981.5406

[Robert.powell@ncosc.net](mailto:Robert.powell@ncosc.net)

**Gwen Canady**  
Chief Deputy State Controller  
919.981.5405

[Gwen.canady@ncosc.net](mailto:Gwen.canady@ncosc.net)

**Lowell Magee**  
BEACON Program Director  
919.431.6511

[Lowell.magee@ncosc.net](mailto:Lowell.magee@ncosc.net)

STATE OF NORTH CAROLINA  
Office of the State Controller

Phone: 919.981.5454

Fax: 919.981.5567

E-mail: [beacon@ncosc.net](mailto:beacon@ncosc.net)

Web: [www.beacon.nc.gov](http://www.beacon.nc.gov)